Università di Pisa

Dipartimento di Informatica

Corso di Laurea Triennale in Informatica

Studio delle Economie di Stablecoin: un'Analisi Basata su Grafi

Candidato:

Simone Morrone

Relatori/Relatrici:

Prof.ssa Laura Emilia Maria Ricci

Dott. Matteo Loporchio

Anno Accademico 2023-2024

Indice

Capitolo 1

Introduzione

L'introduzione delle blockchain pubbliche, come Bitcoin ed Ethereum, ha inaugurato una nuova era per la tecnologia e la finanza, offrendo un modello di gestione di transazioni completamente decentralizzato e trasparente. Basate su registri distribuiti e immutabili, queste reti consentono a ogni nodo di verificare e registrare transazioni senza bisogno di un'autorità centrale. Attualmente, Ethereum occupa la seconda posizione per capitalizzazione di mercato dopo Bitcoin e si distingue per la sua capacità di supportare gli *smart contract*: programmi che operano autonomamente sulla blockchain. Questa funzionalità ha abilitato la creazione di *applicazioni decentralizzate (DApps)* per una vasta gamma di settori, tra cui la *finanza decentralizzata (DeFi)* e la gestione di risorse digitali, aprendo la strada a un ecosistema di servizi che operano senza intermediari e con elevati livelli di sicurezza e trasparenza [1].

Un aspetto fondamentale nello sviluppo di Ethereum è stato l'introduzione dei *token digitali*, strumenti che rappresentano asset o diritti trasferibili tra gli utenti sulla blockchain. Ethereum supporta vari tipi di token, tra cui i più rilevanti sono *ERC-20* per i token *fungibili* e gli *ERC-721* per i token *non fungibili (NFT)*. I token ERC-20, fungibili e intercambiabili, rappresentano unità di valore che possono essere scambiate facilmente, similmente a una valuta tradizionale. Il termine fungibile si riferisce alla capacità di un bene di essere scambiato o sostituito con un altro dello stesso tipo e valore. Al contrario, i token non fungibili (NFT), conformi allo standard ERC-721, sono unici e non intercambiabili; ciascuno possiede caratteristiche distintive che lo rendono differente da ogni altro, rendendoli ideali per rappresentare beni digitali esclusivi, come opere d'arte virtuali, oggetti da collezione, oggetti scambiabili nei videogiochi. Ogni NFT è unico e non può essere sostituito o scambiato con un altro allo stesso valore, creando così nuove opportunità per la proprietà digitale e la collezionabilità.

Tra i token ERC-20, un ruolo di particolare rilievo è svolto dalle **stablecoin**, una categoria specifica di token progettata per affrontare la volatilità delle criptovalute.

A differenza delle criptovalute tradizionali, il valore delle stablecoin è ancorato a un asset di riferimento, come valute fiat o criptovalute. La loro stabilità li rende ideali come mezzo di scambio e riserva di valore, consentendo agli utenti di effettuare transazioni su larga scala, utilizzare protocolli di risparmio e di prestito, senza essere esposti alla volatilità del mercato cripto. Le stablecoin possono essere classificate in tre categorie principali, a seconda del meccanismo che utilizzano per mantenere il loro ancoraggio:

- **Collateralizzate con fiat**: Supportate da riserve centralizzate di valuta fiat, come dollari o euro, detenute da enti che garantiscono la parità 1:1 con l'asset sottostante.
- **Collateralizzate con criptovalute**: Basaste su collaterali decentralizzati, gestiti tramite smart contract, che richiedono sovra-collateralizzazione per compensare la volatilità delle criptovalute utilizzate come garanzia.
- **Algoritmiche**: Mantenute stabili senza collaterali fisici, utilizzando algoritmi che regolano dinamicamente l'offerta in base alla domanda di mercato.

Un tratto distintivo delle blockchain pubbliche è la loro *trasparenza*: ogni transazione è registrata e visibile a chiunque, fornendo una mole di dati senza precedenti per l'analisi scientifica. Questa caratteristica ha reso possibile lo studio delle dinamiche economiche e sociali in un ambiente decentralizzato, consentendo di tracciare i flussi di valore, identificare "hub" di transazione e analizzare le relazioni tra utenti. In particolare, nel caso delle stablecoin, l'analisi delle transazioni può rivelare come questi token siano utilizzati e come si formino e si evolvano le reti di scambio nel tempo, evidenziando i pattern di comportamento all'interno dell'ecosistema DeFi. Rappresentare queste reti di transazioni come grafi risulta particolarmente efficace per analizzarne la struttura e l'evoluzione. In un grafo, infatti, i nodi possono rappresentare gli indirizzi degli utenti o degli smart contract, mentre gli archi orientati rappresentano i trasferimenti di token tra gli indirizzi. Questa rappresentazione consente di visualizzare le interazioni economiche su larga scala in modo intuitivo facilitando l'applicazione di metriche di rete e analisi topologiche. Inoltre la possibilità di osservare la rete ad intervalli di tempo regolari consente di osservare come i pattern di interazione evolvano, offrendo una prospettiva dinamica sulle fluttuazioni dei flussi di valore e sui cambiamenti comportamentali degli utenti.

Motivati da queste ragioni, in questa tesi studiamo le proprietà delle prime quattro reti di token ERC-20 per numero di trasferimenti. Questi token comprendono tre stablecoin e un token "wrappato", derivato da Ether (ETH), la criptovaluta nativa di Ethereum, appositamente creato per garantire la compatibilità con lo standard ERC-20, essendo ETH stato introdotto prima della definizione di tale standard. Tra i token analizzati, il primo è Tether USD (USDT), una stablecoin fiat-collateralizzata

nonché la prima stablecoin sul mercato che, oltre a registrare un numero elevatissimo di trasferimenti, vanta una capitalizzazione di mercato significativa, pari a circa 123 miliardi di dollari. Segue Wrapped Ether (WETH), un token wrappato derivato da ETH, con una capitalizzazione di mercato di circa 9 miliardi di dollari. Completano la lista dei quattro token per numero di trasferimenti, due stablecoin: USD Coin (USDC), con una capitalizzazione di mercato di circa 37.3 miliardi di dollari, e DAI Stablecoin (DAI), che registra una capitalizzazione di mercato di circa 3.3 miliardi di dollari.

Per raccogliere informazioni sui trasferimenti, utilizziamo i dati dei primi 15 milioni di blocchi di Ethereum, che coprono il periodo tra il 30 luglio 2015 e il 21 giugno 2022. In particolare, sfruttiamo le ricevute delle transazioni Ethereum, che includono informazioni sugli eventi di trasferimento ERC-20. Infatti, tali eventi servono come meccanismo principale per notificare ai partecipanti i trasferimenti di token, registrando il mittente, il destinatario e la quantità di token trasferiti. Inoltre per ogni trasferimento viene salvato l'istante in cui è avvenuto, il "*timestamp*", che ha permesso di identificare il periodo temporale di ogni trasferimento. Il timestamp è il tempo in base al numero di secondi trascorsi dalle 00:00:00 UTC del 1° gennaio 1970, l'epoca Unix.

Il nostro contributo principale è articolato come segue. Per ogni token, abbiamo costruito un grafo globale che rappresenta tutte le transazioni registrate durante l'intero periodo analizzato. Ogni grafo globale è diretto, e associa a ciascun arco due pesi: il valore della transazione e il timestamp, che forniscono informazioni aggiuntive oltre al semplice trasferimento tra due indirizzi. Successivamente, le transazioni di ogni token sono state suddivise in finestre temporali mensili utilizzando i timestamp di ogni transazione. Per ogni lista di transazioni estratta, abbiamo costruito una serie di grafi temporali attraverso un processo di *collassamento degli archi*, che elimina i multiarchi (ovvero, transazioni multiple nella stessa direzione tra una coppia di nodi). Il collassamento degli archi è stato necessario per garantire la compatibilità con le librerie utilizzate per l'analisi, come *Igraph* [2] e *WebGraph* [3]. Il risultato è un grafo diretto pesato senza la presenza di multiarchi, dove ogni arco conserva due pesi:

- La *molteplicità dell'arco*, ovvero il numero totale di archi originali tra due nodi.
- La *somma complessiva dei valori trasferiti* in tutte le transazioni associate.

Questo approccio consente di preservare informazioni fondamentali per le analisi effettuate, riducendo al contempo la complessità del grafo. Inoltre, per alcune statistiche, è stato utile collassare anche il grafo globale per ogni token, applicando lo stesso procedimento utilizzato per i grafi temporali.

Successivamente, utilizziamo i grafi prodotti per analizzare l'andamento del numero di nodi e archi come prima misura per comprendere la dimensione e la comples-

sità delle reti associate ai token. Questa analisi introduttiva ci permette di osservare l'evoluzione delle reti nel tempo, identificando variazioni strutturali che possono riflettere cambiamenti nei modelli d'uso, nella popolarità dei token o in eventi specifici di mercato. Approfondiamo inoltre le proprietà topologiche delle reti esaminando metriche come la connettività, la distribuzione dei gradi e delle forze, dove la forza indica il grado ponderato, la transitività, la densità, la reciprocità, l'assortatività e il diametro. Queste metriche forniscono indizi cruciali sul comportamento della rete. Ad esempio, una bassa reciprocità, potrebbe indicare che la rete è dominata da flussi unidirezionali, mentre un'elevata transitività suggerisce la presenza di comunità interconnesse nella rete.

Per motivare il ruolo centrale dei nodi che influenzano la rete, abbiamo pensato di studiare proprietà di centralità, analizzando metriche come il PageRank, gli Hub e Authority score e l'harmonic centrality. Queste analisi ci aiutano a identificare i nodi più influenti nella rete, sia a livello globale che in intervalli specifici. Ad esempio, nelle reti di stablecoin, i nodi centrali possono corrispondere a grandi exchange o wallet con alta attività, mentre nella rete di WETH potrebbero emergere smart contract legati a protocolli DeFi.

Confrontare le metriche tra i grafi globali e temporali è cruciale per comprendere come le reti si trasformano nel corso del tempo. Anche se parliamo principalmente di stablecoin e di un token wrappato, ciascun token rappresenta dinamiche economiche e comportamentali uniche. Ad esempio, le stablecoin fungono spesso da mezzo di scambio o riserva di valore. Tuttavia, il loro utilizzo varia: alcune possono essere più impiegate per transazioni ad alta frequenza, altre per scopi di risparmio o liquidità. Studiare le differenze tra le reti permette di individuare schemi specifici che caratterizzano l'uso di ciascun token, come la formazione di hub centrali, la frammentazione della rete o la concentrazione del flusso di valore in nodi particolari.

Struttura della tesi

Il presente lavoro di tesi è stato strutturato seguendo un ordine logico dei concetti, al fine di garantire chiarezza e coerenza nell'esposizione. Inizialmente, vengono introdotte le basi teoriche delle metriche e delle metodologie adottate, per consentire al lettore di comprendere appieno i fondamenti delle analisi successive. Vengono quindi presentati i risultati sperimentali, accompagnati da un'interpretazione approfondita e contestualizzata, offrendo una visione completa e sistematica del fenomeno analizzato. Di seguito un elenco che spiega in breve il contenuto di questi capitoli:

- **Capitolo 2: Background**: Qui viene spiegata l'importanza della blockchain, della sua trasparenza e di come funziona. Successivamente si parla della blockchain di Ethereum, di come funziona, il suo meccanismo del Gas e la sua

criptovaluta nativa Ether. Si introducono gli smart contract e lo standard ERC-20, che caratterizzano i token analizzati.

- **Capitolo 3: Stablecoin**: Viene spiegato nel dettaglio il funzionamento di una stablecoin con le sue categorie. Viene motivata la scelta dei token di analisi che vengono quindi spiegati individualmente. Inoltre viene introdotto uno scenario di funzionamento scorretto di stablecoin, evidenziando le loro fragilità. Infine viene data una panoramica del loro utilizzo nel mercato decentralizzato.

- **Capitolo 4: Struttura dei grafi per ERC-20**: Qui viene spiegato il processo di modellazione e creazione dei grafi per le transazioni, sia globali che temporali. Vengono poi spiegate brevemente le librerie utilizzate per l'analisi, ovvero WebGraph e Igraph.

- **Capitolo 5: Framework per l'analisi**: Prima di procedere con l'analisi vera e propria, in questo capitolo vengono spiegate tutte le metriche calcolate sui grafi, cercando di far comprendere sia il concetto teorico in letteratura per poi associarlo al nostro contesto di analisi. Il tutto include esempi specifici, per alcune metriche, per una comprensione più improntata all'analisi successiva.

- **Capitolo 6: Risultati sperimentali**: In questo capitolo avviene l'analisi di tutti i risultati ottenuti. Viene spiegato il dataset utilizzato. Successivamente comprende l'analisi strutturale e topologica delle reti. Infine si analizza la centralità per comprendere come nodi chiave influiscono sulla struttura della rete.

- **Capitolo 7: Discussione dei risultati**: In questo capitolo si discutono dettagliatamente i risultati sperimentali ottenuti dalle analisi del capitolo precedente. Si integrano le analisi topologiche con quelle delle centralità e grazie all'individuazione dei nodi più centrali, si motivano le proprietà strutturali delle reti analizzate. Inoltre si confrontano i risultati ottenuti con alcuni risultati simili in letteratura, confutando o confermando quanto ottenuto.

- **Capitolo 8: Conclusioni e Sviluppi futuri**: In questo capitolo si traggono le conclusioni sul lavoro svolto nella tesi con sviluppi futuri.

Capitolo 2

Background

2.1 Blockchain

La blockchain rappresenta una delle innovazioni più rivoluzionarie nell'ambito delle tecnologie digitali contemporanee. Introdotta per la prima volta nel 2008 da Satoshi Nakamoto con il suo celebre whitepaper *Bitcoin: A Peer-to-Peer Electronic Cash System* [4], la blockchain si è presto affermata come la base tecnologica per la gestione sicura e decentralizzata di transazioni e dati, non solo nel settore delle criptovalute, ma anche in numerosi altri ambiti.

In sostanza, una blockchain è un registro distribuito, immutabile e decentralizzato, che consente la registrazione cronologica di transazioni in una catena di blocchi interconnessi attraverso hash crittografici. Ogni blocco è identificato univocamente da un *hash* crittografico, che lo collega al blocco successivo, formando una catena continua e inalterabile. All'interno di un blocco, sono memorizzati dati essenziali come il timestamp, l'hash del blocco precedente e le transazioni approvate tramite il meccanismo di consenso.

2.1.1 Immutabilità, Decentralizzazione e Trasparenza

La blockchain garantisce l'*immutabilità* delle transazioni grazie alla sua struttura crittografica. Ogni blocco nella catena contiene un *hash univoco*[1] del blocco precedente, creando un legame tra i blocchi che ne assicura l'integrità dei dati. Questo meccanismo impedisce che le informazioni archiviate possano essere modificate senza alterare anche tutti i blocchi successivi, rendendo evidente qualsiasi tentativo di manomissione. Pertanto, una volta che una transazione viene registrata all'interno

[1] Valore alfanumerico generato da un algoritmo di hashing crittografico che prende una transazione e produce un output di lunghezza fissa.

di un blocco, essa diventa immutabile e permanentemente parte della storia della rete.

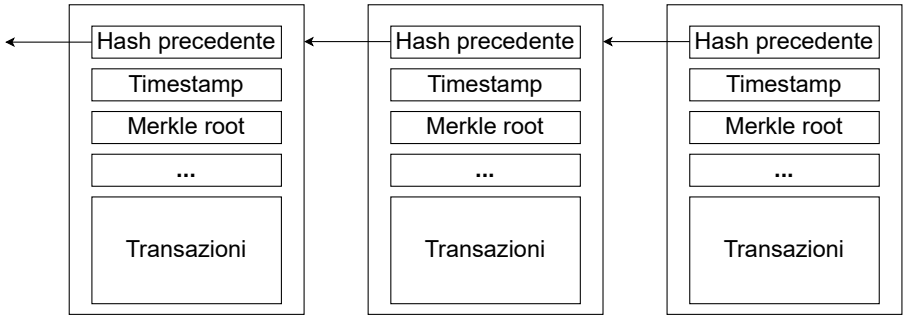


Figura 2.1: Block Chaining

In Figura 2.1, è evidente come gli *hash* dei blocchi precedenti, il timestamp e la *Merkle root* [5] delle transazioni siano interconnessi. La Merkle root è la radice di un *Merkle tree*, una struttura dati ad albero che organizza e verifica l'integrità delle transazioni in modo efficiente e sicuro. Ogni nodo foglia del Merkle tree rappresenta l'hash crittografico di una singola transazione, mentre i nomi intermedi vengono calcolati combinando e "hashando" i valori dei nodi figli. Questo processo continua fino a raggiungere la radice, che funge da impronta digitale univoca per l'intero insieme di transazioni. Una modifica a qualsiasi transazione comporterebbe la necessità di ricalcolare non solo l'hash del nodo modificato, ma anche quelli di tutti i nodi lungo il percorso fino alla Merkle root. Questo meccanismo garantisce l'integrità delle transazioni del blocco, poiché ogni alterazione viene immediatamente rilevata. Inoltre, essendo la Merkle root inclusa nell'hash del blocco stesso, qualsiasi modifica richiederebbe il ricalcolo dell'hash del blocco corrente e di tutti quelli successivi, invalidando l'intera catena. Questo rende la blockchain altamente resistente a modifiche non autorizzate, rafforzando ulteriormente la fiducia nel sistema.

Oltre alla sua immutabilità, la blockchain è strutturalmente **decentralizzata**, nel senso che non esiste un'autorità centrale che ne garantisce il funzionamento. Ogni nodo nella rete conserva una copia completa e aggiornata della blockchain, eliminando la necessità di una figura decentralizzata per validare le transazioni. Questa decentralizzazione distribuisce il controllo tra tutti i partecipanti della rete, riducendo il rischio di corruzione e manomissioni da parte di un singolo ente. Tuttavia è importante ricordare che la decentralizzazione, se mal gestita o applicata in modo non appropriato, può presentare rischi di potenziali inefficienze. È quindi cruciale trovare un equilibrio che permetta di mantenere la sicurezza e la trasparenza senza introdurre vulnerabilità strutturali.

Infine, la blockchain pubblica garantisce anche un alto livello di trasparenza. Su reti come Bitcoin ed Ethereum, ogni transazione è visibile a tutti i partecipanti

della rete, senza compromettere la privacy, poiché l'utilizzo di indirizzi, ottenuti come hash della chiave pubblica, protegge le identità personali. Questo approccio assicura una tracciabilità totale, permettendo a chiunque di verificare l'autenticità e la correttezza delle operazioni registrate.

2.1.2 Algoritmi di consenso

Uno degli aspetti centrali della blockchain è l'assenza di un'autorità centrale: la validazione delle transazioni avviene attraverso un meccanismo di consenso, che varia a seconda della blockchain. Gli algoritmi di consenso determinano quale sarà il prossimo insieme di transazioni (e quindi il prossimo blocco) ad essere aggiunto alla blockchain. Ogni validatore propone un proprio insieme di transazioni e l'algoritmo di consenso sceglie quale di questi blocchi sarà aggiunto alla catena, in base a criteri che variano l'algoritmo utilizzato. Ad esempio, nel caso di Bitcoin, la *Proof of Work (PoW)* richiede che i nodi della rete, chiamati *miner*, competano per risolvere complessi problemi crittografici. Questo processo non solo garantisce la sicurezza della rete, ma rende anche estremamente difficile manipolare i dati. Tuttavia, la PoW è nota per il suo elevato consumo energetico, motivo per cui nuove blockchain come Ethereum stanno migrando verso meccanismi più efficienti come il *Proof of Stake (PoS)*.

Nella PoS [6], i validatori vengono selezionati in base alla quantità di criptovaluta in loro possesso, riducendo drasticamente il consumo energetico. Anziché basarsi sulla potenza di calcolo, nel meccanismo PoS la probabilità di essere scelti per aggiungere un blocco dipende dalla quantità di monete detenute rispetto al totale in circolazione. Gli utenti con maggiori quote hanno un interesse diretto nel mantenere la rete sicura, poiché il valore della criptovaluta posseduta perderebbe valore in caso di attacchi. Un attaccante, per compromettere la rete, dovrebbe possedere la maggior parte della valuta, un'operazione impraticabile e controproducente, dato che ridurrebbe il valore della criptovaluta stessa.

2.2 Ethereum

Ethereum è una piattaforma blockchain decentralizzata creata nel 2013 da *Vitalik Buterin* [7] per affrontare i limiti della blockchain di Bitcoin. Mentre Bitcoin si concentra principalmente sul trasferimento di valore tramite transazioni finanziarie, Ethereum estende questo concetto introducendo la possibilità di eseguire *smart contract* (Sezione 2.4) e sviluppare applicazioni *decentralizzate* (DApps).

Gli smart contract sono veri e propri programmi, scritti in un linguaggio di programmazione Turing-completo. Questa caratteristica consente agli smart contract

di gestire una vasta gamma di operazioni, dalla semplice verifica di una transazione alla gestione di processi più complessi, senza la necessità di intermediari.

Il progetto Ethereum non solo conserva i vantaggi della tecnologia blockchain, come la *decentralizzazione* e la *trasparenza*, ma aggiunge una nuova dimensione programmabile alla rete, rendendo Ethereum molto più flessibile e versatile rispetto a Bitcoin. Nel 2014, con la fondazione di *Ethereum Foundation*, fu organizzata una raccolta fondi attraverso la vendita di *Ether (ETH)*, la criptovaluta nativa di Ethereum. A differenza di Bitcoin, Ether non si limita a fungere da riserva di valore, ma è utilizzato per pagare le commissioni di transazione e per gestire le risorse computazionali necessarie per eseguire le applicazioni e i contratti intelligenti sulla rete. Dopo una fase di iniziale di sviluppo e testing, Ethereum fu ufficialmente lanciato nel luglio 2015 con la versione *Frontier* [1], che segnò l'inizio di un nuovo paradigma per l'ecosistema blockchain, con la possibilità di costruire applicazioni decentralizzate senza la necessità di un'autorità centrale.

2.2.1 La criptovaluta di Ethereum

L'Ether è la criptovaluta nativa della piattaforma Ethereum, utilizzata per incentivare i miner e, nella *Proof of Stake (PoS)*, per ricompensare i validatori che contribuiscono alla sicurezza e alla manutenzione della rete. Gli utenti pagano il **gas** (Sezione 2.2.3), misurato in Ether, per effettuare transazioni o eseguire operazioni più complesse, come l'interazione con gli smart contract. Questo meccanismo garantisce l'efficienza della rete e impedisce che operazioni malintenzionate o troppo onerose la sovraccarichino.

A differenza di Bitcoin, che ha un'offerta massima predefinita, Ethereum non ha un limite rigido alla quantità totale di Ether in circolazione. Questo rende la gestione dell'offerta più flessibile, ma potenzialmente soggetta a inflazione. Tuttavia, con l'implementazione del protocollo EIP-1559 nel 2021, una parte delle commissioni di transazione viene "bruciata" (ovvero eliminata dal sistema), il che riduce l'inflazione e migliora la scarsità dell'Ether [8].

2.2.2 La Ethereum Virtual Machine

La *Ethereum Virtual Machine (EVM)* è una macchina virtuale decentralizzata che esegue smart contract e transazioni su Ethereum. Funziona come un ambiente di esecuzione decentralizzato per il codice distribuito sulla rete. Ogni nodo della rete esegue una propria copia della EVM, assicurando che ogni smart contract sia eseguito in modo coerente e sicuro.

La EVM gestisce le risorse computazionali tramite un sistema di gas, che determina il costo di ogni operazione eseguita. Le transazioni e i contratti intelligenti richiedono una quantità specifica di gas per essere eseguiti, pagato in ETH.

Dal punto di vista dell'architettura, la EVM è progettata per essere Turing-completa[2], il che significa che può eseguire qualsiasi calcolo computabile, a condizione che ci siano risorse computazionali sufficienti (gas).

2.2.3 Gas

Il *gas* è l'unità che misura la quantità di sforzo computazionale necessario per eseguire operazioni specifiche sulla rete Ethereum. Ogni operazione eseguita nella EVM richiede una quantità specifica di gas. Questo meccanismo esiste per evitare l'uso improprio della rete, poiché ogni contratto o transazione deve pagare per le risorse computazionali che consuma.

Quando si invia una transazione, vengono specificati:

1. *Limite del gas (STARTGAS)*: La quantità massima di gas che l'utente è disposto a spendere. Se il limite è insufficiente, l'operazione fallisce e viene annullata, come se non fosse mai avvenuta, ma il gas consumato fino a quel punto non viene restituito.

2. *Prezzo del gas (GASPRICE)*: L'importo in ETH che l'utente è disposto a pagare per ogni unità di gas. Le transazioni con prezzi del gas più alti avranno priorità sulle altre.

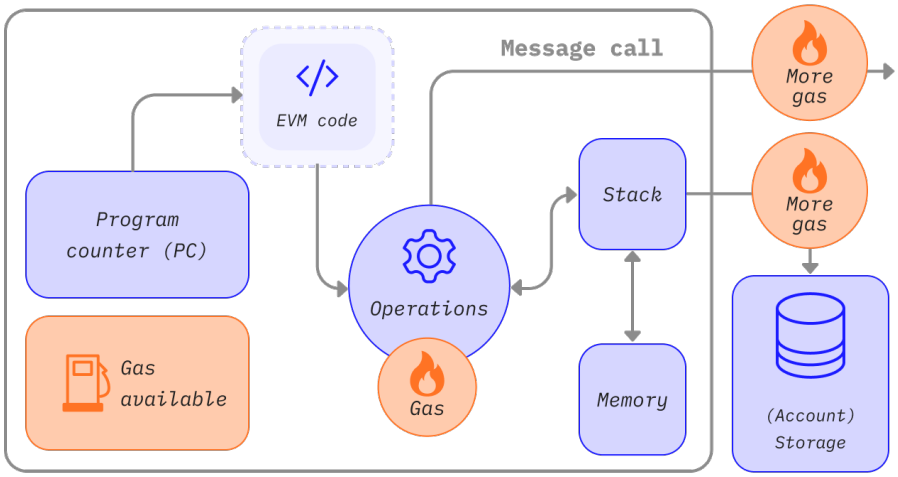


Figura 2.2: Flusso di esecuzione di una transazione all'interno della EVM [9]

[2]Sistema che può eseguire qualsiasi calcolo algoritmico, purché disponga di tempo e risorse sufficienti.

La Figura 2.2 mostra il flusso di esecuzione di una transazione o smart contract all'interno della EVM. Il Program Counter (PC) tiene traccia dell'istruzione corrente, mentre il gas indica la quantità di risorse computazionali ancora disponibili. Le operazioni eseguite consumano gas, che viene dedotto durante l'elaborazione. Se la transazione richiedesse ulteriori operazioni, viene consumato più gas, come mostrato nella parte destra dell'immagine [10].

2.3 Ciclo di vita di una transazione in Ethereum

Il ciclo di vita di una transazione in Ethereum è un processo fondamentale che permette alla rete di mantenere il proprio stato aggiornato. Ogni transazione, sia essa un trasferimento di ETH o l'interazione con uno smart contract, porta a un cambiamento nello stato globale della rete Ethereum, influenzando direttamente gli account coinvolti. Prima di descrivere il ciclo di vita di una transazione, è utile chiarire le tipologie di account presenti in Ethereum e come interagiscono con le transazioni.

2.3.1 Tipi di Account: EOA e Smart Contract

In Ethereum esistono due tipi di account: *account esterni* (o EOA, *External Owned Accounts*) e *smart contract*. Gli EOA sono identificati dalla loro chiave *pubblica*, derivata crittograficamente da una chiave *privata*. Il possesso della chiave privata corrispondete consente al proprietario di firmare digitalmente transazioni, che possono trasferire ETH o interagire con gli smart contract. La creazione di un EOA è gratuita e non richiede gas, poiché consiste semplicemente nela generazione di una coppia di chiavi tramite l'algoritmo ECDSA [11], utilizzato anche da Bitcoin. Invece, gli smart contract non sono controllati da individui, ma eseguono codice predefinito sulla blockchain e vengono creati tramite transazioni speciali. A differenza degli EOA, la creazione di uno smart contract comporta un costo di gas, poiché implica l'aggiunta di codice eseguibile alla rete.

Gli account Ethereum hanno quattro campi principali: il **nonce**, che tiene traccia del numero di transazioni inviate dall'account; il **balance**, che rappresenta il saldo in *"wei"* (unità base di Ether, dove 1 ETH = 10^{18} wei); il **codeHash**, che contiene il riferimento al codice eseguibile associato all'account (nel caso dei contratti); e lo **storageRoot**, che rappresenta l'hash di un *Merkle Patricia Trie* che codifica lo spazio di archiviazione del contratto. Il Merkle Patricia Trie è una struttura dati utilizzata da Ethereum per memorizzare lo stato globale della rete, inclusi i saldi degli account e i dati degli smart contract. Combina un Merkle Tree con un Patricia Trie [12], permettendo un accesso efficiente ai dati e garantendo la loro integrità e verifica crittografica.

2.3.2 Fasi del ciclo di vita di una transazione

Una transazione inizia quando un *EOA* firma digitalmente una richiesta e la invia alla rete Ethereum. Le transazioni includono il mittente, il destinatario, la quantità di Ether da trasferire, un eventuale campo per interagire con smart contract, e due valori fondamentali: *STARTGAS* e *GASPRICE* (Sezione 2.2.3).

Dopo l'invio, la transazione viene propagata nella rete *peer-to-peer* di Ethereum. I validatori ricevono la transazione e la inseriscono nella loro *transaction pool*, un'area che contiene tutte le transazioni in attesa di essere incluse in un blocco[3]. Durante il processo di validazione, i nodi selezionano le transazioni in base al valore del GASPRICE: quelle con prezzi più elevati vengono elaborate con priorità, poiché forniscono ai validatori ricompense maggiori.

Una volta che una transazione viene scelta ed eseguita, il nodo verifica la sua validità controllando, ad esempio, la firma del mittente e se il *nonce* e il saldo sono corretti. Se tutto è in regola, il saldo dell'account mittente viene ridotto dell'importo specificato più le commissioni di gas, e l'account destinatario riceve l'importo in Ether. Nel caso di un'interazione con uno smart contract, la Ethereum Virtual Machine (EVM) carica ed esegue il codice associato al contratto, consumando gas per ogni operazione.

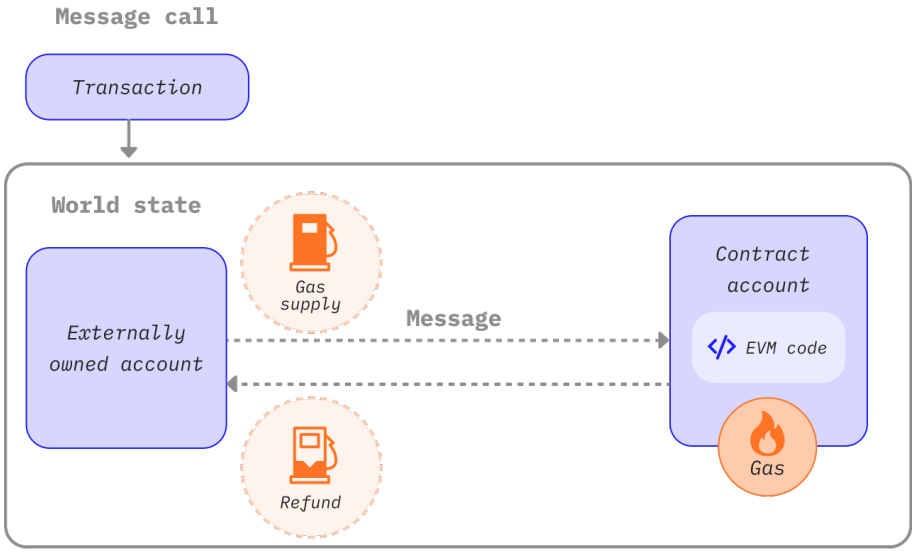


Figura 2.3: Rappresentazione come un EOA avvia una transazione [9]

Se la transazione esaurisce il gas prima che tutte le operazioni siano completate, viene annullata e lo stato della rete ritorna a quello precedente l'esecuzione, ma

[3]La *transaction pool* è uno spazio temporaneo gestito dai nodi Ethereum dove le transazioni firmate, ma non ancora confermate, sono archiviate.

il gas consumato fino a quel momento non viene restituito. Questo meccanismo è fondamentale per prevenire un uso incontrollato di risorse computazionali e garantire che operazioni inefficienti o mal progettate non blocchino la rete.

La Figura 2.3 mostra come un EOA avvii una transazione, fornendo il gas necessario per eseguire operazioni su un *contract account*. La EVM esegue il codice del contratto e, se il gas non si esaurisce prima del completamento, il saldo rimanente viene rimborsato all'EOA.

2.3.3 Tipologie di Transazione

Esistono due principali tipologie di transazione:

1. *Transazione di trasferimento di valore*: in questo caso, un EOA trasferisce Ether a un altro account, sia esso un altro EOA o un account di contratto. Questa transazione aggiorna semplicemente il saldo degli account.

2. *Creazione o invocazione di un contratto*: nel caso della creazione di un contratto, l'input della transazione contiene il bytecode[4] che sarà eseguito dalla EVM per creare un nuovo smart contract. Una volta distribuito, il contratto è identificato da un indirizzo univoco e può essere invocato da altre transazioni per eseguire operazioni predefinite.

2.4 Smart Contract

Gli **smart contract** sono un'innovazione fondamentale introdotta dalla blockchain di Ethereum, concepita per automatizzare l'esecuzione di contratti tramite un sistema decentralizzato e immutabile. Si tratta di programmi che eseguono automaticamente le istruzioni predefinite nel loro codice, ma solo quando vengono attivati da una transazione inviata da un utente o da un altro smart contract. Questo elimina il bisogno di intermediari o autorità centrali, garantendo trasparenza e fiducia nel processo. Il concetto di smart contract è stato teorizzato da *Nick Szabo* negli anni '90, definendolo come *"a computerised transaction protocol that executes the terms of a contract"* [13]. Tuttavia ha trovato la sua piena realizzazione con l'introduzione di Ethereum, che ha reso possibile la programmabilità delle transazioni.

La struttura tecnica degli smart contract è basata su un linguaggio di programmazione specifico, come *Solidity* [14], e una volta creati, vengono compilati in *bytecode* e distribuiti sulla rete Ethereum. Una volta distribuito, uno smart contract

[4]Formato binario del codice eseguibile di uno smart contract sulla EVM. Ottimizzato per essere interpretato dalla macchina virtuale, rendendo possibile l'esecuzione automatica delle operazioni definite nel contratto senza ulteriori traduzioni.

diventa immutabile, il che significa che né il creatore né altre parti possono modificarlo. Questo garantisce sicurezza e trasparenza, ma introduce anche complessità, come la necessità di eseguire una verifica rigorosa del codice prima della distribuzione.

Dal punto di vista operativo, gli smart contract su Ethereum funzionano all'interno della EVM, che esegue le istruzioni in modo distribuito sui nodi della rete. La transazione che innesca uno smart contract richiede l'utilizzo di gas per limitare le risorse utilizzate dalle operazioni.

Gli smart contract trovano applicazione in una vasta gamma di settori, dalla finanza decentralizzata (DeFi), alla gestione della proprietà intellettuale, fino alla creazione di token e NFT. Grazie alla loro capacità di operare in modo decentralizzato e senza intermediari, gli smart contract riducono i costi operativi e aumentano la fiducia nei processi contrattuali [15]. Tuttavia, non sono esenti da problematiche: vulnerabilità come gli attacchi *re-entrancy*[5] o errori di codifica hanno messo in luce la necessità di rigorosi controlli di sicurezza e revisione del codice [16].

2.4.1 Funzionamento degli smart contract

L'esecuzione di uno smart contract avviene tramite una transazione, che rappresenta l'invocazione di una funzione del contratto. Questa transazione può includere molteplici istruzioni e, una volta completata, viene registrata in modo immutabile nella blockchain. Una volta soddisfatte le condizioni predefinite in uno smart contract, il codice viene eseguito in modo deterministico, garantendo che le istruzioni siano eseguite secondo quanto programmato. L'intero ciclo di vita degli smart contract è costituito da quattro fasi consecutive illustrato nella Figura 2.4

1. **Creazione**: Le parti coinvolte definiscono i termini contrattuali che possono riguardare obblighi, diritti o condizioni programmatiche. Dopo aver concordato la logica operativa, gli sviluppatori la traducono in uno smart contract scritto spesso in Solidity. È importante notare come varia la tipologia degli smart contract: spesso sono contratti legali come possono essere anche semplici espressioni di logica programmatica per l'esecuzione automatizzata di funzioni o transazioni sulla blockchain. La creazione è un processo iterativo che coinvolge più cicli di negoziazione e validazione, simile allo sviluppo di software tradizionali.

2. **Distribuzione**: Lo smart contract validato viene distribuito sulla block-chain, dove diventa immutabile. Qualsiasi modifica richiede la creazione di un nuovo contratto. Durante questa fase, le risorse digitali delle parti coinvolte vengono

[5]Vulnerabilità emersa con l'attacco famoso al DAO nel 2016 dove un contratto malevolo sfrutta una funzione esterna per chiamare ripetutamente un contratto vulnerabile prima che quest'ultimo possa aggiornare il suo stato interno.

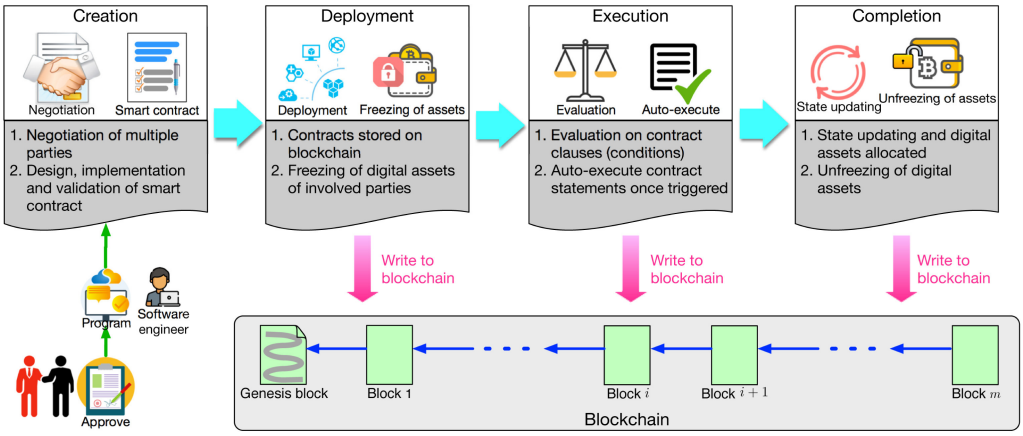


Figura 2.4: Ciclo di vita di uno smart contract [17]

bloccate nei portafogli digitali, impedendo trasferimenti fino al completamento del contratto.

3. **Esecuzione**: Quando le condizioni specificate nel contratto vengono soddisfatte (ad esempio, la ricezione di un prodotto), le funzioni contrattuali vengono eseguite automaticamente. Queste operazioni generano transazioni, che vengono verificate dai miner e registrate nella blockchain. Ogni transazione corrisponde all'invocazione di una funzione del contratto, che esegue una serie di istruzioni e può modificare lo stato della blockchain.

4. **Completamento**: Una volta che tutte le operazioni sono state eseguite, gli stati aggiornati delle parti vengono archiviati nella blockchain e le risorse digitali, come il trasferimento di denaro, vengono sbloccate e trasferite tra le parti. Il ciclo di vita dello smart contract si conclude con il completamento delle transazioni e l'aggiornamento dello stato sulla blockchain.

Sebbene gli smart contract offrano un grande potenziale per favorire l'innovazione nei processi aziendali, ci sono ancora diverse sfide da superare. Tra queste sfide rientrano problemi di privacy e sicurezza, in quanto i dati delle transazioni su blockchain sono visibili a tutti i partecipanti alla rete, esponendo potenzialmente informazioni sensibili. Inoltre, vi sono vulnerabilità funzionali, come gli attacchi di re-entrancy, che consentono a un attore malevolo di sfruttare chiamate ripetute a una funzione per sottrarre fondi. Anche la correttezza del codice è una sfida critica: una volta distribuito, uno smart contract non può essere modificato, quindi eventuali errori possono avere conseguenze significative. Infine, la dipendenza dall'ordine delle transazioni può causare risultati incoerenti se le transazioni vengono eseguite in un ordine non previsto [17].

2.5 Token fungibili (ERC-20)

Dopo aver esplorato il funzionamento degli smart contract e il loro ruolo cruciale nel garantire automazione e fiducia all'interno della rete Ethereum, diventa essenziale approfondire una delle loro applicazioni più rilevanti: la creazione e gestione dei **token**. Un token è un'unità digitale di valore che può rappresentare un'ampia gamma di asset o diritti all'interno di una blockchain. I token possono essere utilizzati per rappresentare valute, azioni, proprietà o persino l'accesso a servizi o applicazioni. Il termine fungibile si riferisce alla capacità di un bene di essere scambiato o sostituito con un altro dello stesso tipo e valore. Nel caso dei token ERC-20, ogni token è identico agli altri in termini di valore e funzione, rendendoli intercambiabili tra loro (Sezione 2.5.2). Al contrario, i token non fungibili (NFT) rappresentano oggetti unici e non intercambiabili.

Grazie agli smart contract, Ethereum non solo abilita transazioni, ma permette anche la creazione di standard condivisi per i token digitali [18].

Nel contesto della blockchain di Ethereum, i *token ERC-20* [19] hanno un ruolo centrale rappresentando uno degli standard più utilizzati per la creazione e gestione di asset digitali fungibili. Lo standard ERC-20, proposto nel 2015, è stato sviluppato per risolvere le necessità di uniformità e interoperabilità tra i token, permettendo agli sviluppatori di creare token compatibili con l'intera infrastruttura di Ethereum, inclusi wallet[6], exchange[7] e applicazioni decentralizzate. A differenza dei token nativi di una blockchain, come ETH su Ethereum o *bitcoin (BTC)* su Bitcoin, i token ERC-20 vengono creati all'interno di smart contract e sono gestiti tramite funzioni specifiche definito nello standard.

Un aspetto cruciale dello standard ERC-20 è che esso definisce un insieme di regole e interfacce comuni che ogni token deve seguire. Queste regole includono funzioni per il trasferimento di token, la verifica del saldo e l'approvazione per spostare token per conto di un altro indirizzo. Grazie a questa standardizzazione, i token ERC-20 possono essere facilmente scambiati, integrati e utilizzati su tutte le piattaforme che supportano Ethereum, garantendo così l'interoperabilità e riducendo la complessità per sviluppatori e utenti.

2.5.1 Le specifiche tecniche dello standard ERC-20

Lo standard ERC-20 definisce un insieme di regole e interfacce che tutti i token fungibili su Ethereum devono seguire per garantire l'interoperabilità e la compatibilità all'interno dell'ecosistema. Le specifiche di ERC-20 comprendono sei funzioni

[6] Applicazione o dispositivo hardware utilizzato per gestire chiavi private e pubbliche necessarie per accedere ai fondi su blockchain, inviare e ricevere criptovalute e monitorare il saldo.

[7] Piattaforma online che consente agli utenti di scambiare criptovalute tra loro o con valute tradizionali (fiat).

fondamentali e due eventi che sono implementati all'interno degli smart contract per gestire e tracciare i token. Grazie a questa standardizzazione, sviluppatori e aziende possono creare token che interagiscono facilmente con exchange, wallet e applicazioni decentralizzate, senza la necessità di sviluppare soluzioni personalizzate per ogni progetto.

Funzioni fondamentali

Queste funzioni assicurano che i token seguano le stesse regole di base per quanto riguarda trasferimenti, autorizzazioni e gestione del saldo, facilitando la creazione e il trasferimento di token su Ethereum.

1. `function totalSupply() public view returns (uint256)`: Questa funzione restituisce il numero totale di token esistenti per un dato contratto ERC-20. Definendo l'offerta totale dei token, assicura che il numero massimo di unità circolanti sia trasparente e verificabile.

2. `function balanceOf(address _owner) public view returns (uint256 balance)`: Questa funzione restituisce il saldo di uno smart contract. È cruciale per determinare quanti token possiede un determinato account e viene spesso utilizzata per verificare se un account ha abbastanza token per effettuare una transazione.

3. `function transfer(address _to, uint256 _value) public returns (bool success)`: Questa funzione permette di trasferire un numero specifico di token da un account mittente a un account destinatario. Viene utilizzata per effettuare semplici transazioni dirette tra utenti o applicazioni, spostando token da un indirizzo a un altro. Inoltre l'amount è rappresentato come un intero a 256 bit.

4. `function approve(address _spender, uint256 _value) public returns (bool success)`: Questa funzione consente a un utente di autorizzare un'altra entità (solitamente uno smart contract) a spendere una quantità specifica di token per suo conto. È spesso utilizzata in scenari in cui un'applicazione deve essere in grado di trasferire token per un utente, come negli exchange decentralizzati.

5. `function transferFrom(address _from, address _to, uint256 _value) public returns (bool success)`: Questa funzione esegue il trasferimento di token che sono stati precedentemente approvati con `approve()`. Consente ai contratti di spostare token da un account a un altro senza l'intervento diretto del proprietario, purché l'approvazione sia stata concessa.

6. `function allowance(address _owner, address _spender) public view returns (uint256 remaining)`: Questa funzione restituisce il numero di token che un mittente ha autorizzato un'altra entità a prelevare dal suo saldo tramite `approve()`. È fondamentale per garantire che l'importo autorizzato non venga superato e per verificare i limiti di trasferimento.

Eventi chiave

In Ethereum un *evento* è un meccanismo che permette agli smart contract di notificare determinati cambiamenti di stato all'interno della blockchain. Quando un evento viene emesso, esso genera una notifica che può essere rilevata da utenti, contratti o applicazioni decentralizzate. Questo consente a chi osserva la rete di accorgersi di queste notifiche e, se necessario, eseguire determinate azioni di risposta. Sono molto utili per monitorare le transazioni o le autorizzazioni che avvengono tra account.

Lo standard ERC-20 definisce due eventi cruciali per il monitoraggio delle transazioni e delle autorizzazioni all'interno della blockchain di Ethereum. Questi eventi permettono agli osservatori della rete di tenere traccia dei trasferimenti di token e delle autorizzazioni concesse tra account. L'evento "`Transfer(address indexed from, address indexed to, uint256 value)`", viene emesso ogni volta che avviene un trasferimento di token tra due indirizzi. Questo evento è essenziale per tracciare i movimenti di token nella rete Ethereum e viene utilizzato da exchange e applicazioni per aggiornare i saldi degli utenti in tempo reale. L'evento "`Approval(address indexed owner, address indexed spender, uint256 value)`", viene emesso quando un utente concede l'approvazione a un altro indirizzo per spendere una quantità specifica di token. Questo evento è fondamentale per applicazioni che richiedono l'autorizzazione preventiva degli utenti per eseguire operazioni complesse con i loro token, come nei casi di exchange decentralizzati o contratti di prestito [8].

Modularità e Interoperabilità

Definendo un insieme uniforme di funzioni ed eventi, ERC-20 permette a qualsiasi applicazione o servizio che rispetti lo standard di interagire con i token senza dover sviluppare soluzioni su misura per ogni implementazione. Questo ha portato una rapida diffusione dei token ERC-20 e ha creato un ecosistema interoperabile in cui i token possono essere scambiati, trasferiti e gestiti facilmente tra piattaforme diverse.

[8]Nella blockchain di Ethereum sono smart contract che permettono agli utenti di prendere in prestito o prestare criptovalute senza la necessità di intermediari tradizionali come banche o istituti finanziari. Questi contratti automatizzano il processo di gestione del prestito, stabilendo regole per il tasso di interesse, la durata del prestito e la garanzia, garantendo così maggiore trasparenza e sicurezza nelle transazioni.

2.5.2 I token fungibili: definizione e caratteristiche

Il concetto di **fungibilità** si riferisce alla proprietà di un bene per cui ciascuna unità è identica e può essere scambiata con un'altra dello stesso tipo. Ad esempio, una banconota da 10 euro ha lo stesso valore di un'altra banconota da 10 euro. Questa caratteristica è essenziale per qualsiasi sistema di scambio che richieda uniformità tra le unità scambiate, come avviene nel caso delle valute. Applicata ai token digitali, la fungibilità implica che ogni unità di un token ERC-20 abbia lo stesso valore e possa essere utilizzata e scambiata liberamente all'interno della rete.

Differenza tra token fungibili e non fungibili

Mentre i token ERC-20 rappresentano asset fungibili, i token non fungibili (NFT), standardizzati tramite ERC-721 e successivamente ERC-1155, sono progettati per rappresentare asset unici e non intercambiabili. Questa distinzione è fondamentale per comprendere come i token fungibili siano più adatti per applicazioni che richiedono la rappresentazione di beni omogenei e standardizzati, come le valute digitali, mentre gli NFT sono più indicati per oggetti da collezione, proprietà digitali uniche e arte digitale. Esempi di token non fungibili includono opere d'arte digitali, proprietà immobiliari tokenizzate e asset virtuali nei giochi. Invece, i token fungibili ERC-20 sono utilizzati per rappresentare valute digitali come Tether (USDT), USD Coin (USDC) e Dai (DAI), o per distribuire utility token all'interno di piattaforme decentralizzate.

2.5.3 La gestione delle transazioni ERC-20

Le transazioni ERC-20 rappresentano il cuore del funzionamento dei token fungibili sulla rete Ethereum. Ogni transazione ERC-20 implica il trasferimento di token digitali tra account attraverso uno smart contract, seguendo un insieme standard di regole definite dallo standard ERC-20. Queste transazioni non sono semplici spostamenti di valore come nel caso delle transazioni di Ether, ma richiedono l'interazione con il codice degli smart contract che governa i token. Grazie alla standardizzazione introdotta da ERC-20, i token possono essere trasferiti, scambiati e utilizzati in modo uniforme e interoperabile su tutta la rete Ethereum, permettendo di integrare facilmente funzionalità legate al trasferimento di valore in wallet, exchange decentralizzati (DEX) e applicazioni DeFi.

Le transazioni di token ERC-20, come la chiamata alla funzione `Transfer()`, sono meno costose rispetto a operazioni più complesse, come `TransferFrom()`, che coinvolge anche la gestione di autorizzazioni preesistenti. Tuttavia, i costi di gas possono variare notevolmente a seconda delle condizioni della rete Ethereum. Durante i

periodi di congestione della rete, i costi di gas possono aumentare significativamente, rendendo costose anche le transazioni più semplici.

Le operazioni che coinvolgono token ERC-20 possono essere ottimizzate per ridurre i costi di gas utilizzando soluzioni *Layer 2* (come *Optimism* o *Arbitrum)* [20], che trasferiscono parte del carico computazionale al di fuori della rete principale di Ethereum.

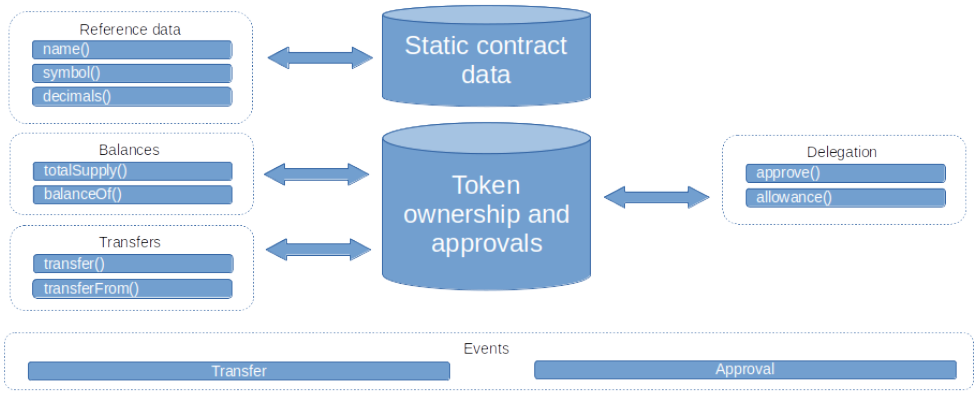


Figura 2.5: Struttura base di un contratto ERC-20 [21]

La Figura 2.5 fornisce una rappresentazione delle principali componenti operative di un contratto ERC-20, illustrando chiaramente come le funzioni e gli eventi precedentemente descritti interagiscano per gestire il trasferimento e la proprietà dei token all'interno della rete Ethereum. Nella parte superiore della Figura troviamo le funzioni statiche del contratto, come `name()`, `symbol()` e `decimals()`, che definiscono gli attributi descrittivi del token, fondamentali per la sua identificazione ma non direttamente coinvolti nelle operazioni di trasferimento. La parte centrale della Figura evidenzia le funzioni che regolano la gestione del saldo e delle transazioni, come `totalSupply()` e `balanceOf()`, fornendo trasparenza sul numero totale di token in circolazione e sul saldo di ogni account. Le funzioni di trasferimento, come `transfer()` e `transferFrom()`, gestiscono le operazioni di movimento dei token tra account, mentre la delegazione delle autorizzazioni è illustrata attraverso le funzioni `approve()` e `allowance()`. Per concludere, nella parte inferiore della Figura sono rappresentati gli eventi `Transfer` e `Approval`, che emettendo notifiche pubbliche che aggiornano lo stato dei trasferimenti sulla blockchain.

Capitolo 3

Stablecoin

Lo standard ERC-20 per i token fungibili ha gettato le basi per la creazione e la gestione di una vasta gamma di asset digitali all'interno della rete Ethereum. Un'altra categoria fondamentale di token digitali sono le **stablecoin**, che sono oggetto di analisi in questa tesi. Questo capitolo è dedicato quindi alla descrizione di questo tipo di coin.

3.1 Introduzione e categorie di stablecoin

Le stablecoin sono una particolare categoria di criptovalute progettate per mantenere un valore stabile, distinguendosi così dalle criptovalute come BTC o ETH, che invece subiscono forti oscillazioni di prezzo. L'idea di base delle stablecoin è quella di offrire una riserva di valore più sicura, spesso ancorata a un asset di riferimento, come una valuta tradizionale, per esempio il dollaro statunitense. Questo le rende molto più adatte per chi vuole utilizzare le criptovalute non solo come mezzo di scambio nelle transazioni quotidiane, ma anche, per proteggere i propri risparmi. Il loro valore rimane infatti legato a un asset stabile offrendo agli utenti la tranquillità di potersi muovere all'interno del mercato delle criptovalute senza il timore di improvvise oscillazioni. Per ottenere questa stabilità, esistono tre principali tipi di stablecoin che differiscono per il modo in cui mantengono l'ancoraggio al valore: stablecoin collateralizzate con fiat, con criptovalute e stablecoin algoritmiche.

3.1.1 Stablecoin collateralizzate con fiat

Le stablecoin collateralizzate con *fiat*[1] sono tra le soluzioni più utilizzate per affrontare la volatilità del mercato delle criptovalute. Sono supportate da riserve di valuta tradizionale, gestite da entità centralizzate, che assicurano la stabilità mantenendo un rapporto di parità con l'asset di riferimento, solitamente il dollaro statunitense in rapporto 1:1. Questo garantisce che il valore del token rimanga stabile, favorendo il loro utilizzo sia come mezzo di pagamento che come riserva di valore. Per ogni token emesso sulla blockchain, vi è una corrispondente quantità di valuta fiat detenuta in riserva. Questo modello implica che un'entità o un consorzio si occupi della gestione delle riserve, assicurando che per ogni stablecoin in circolazione ci sia un equivalente valore in valuta fiat disponibile. Sebbene questa gestione centralizzata contrasti con l'ideale di *decentralizzazione* della blockchain (Sezione 2.1.1), è particolarmente efficace nel garantire la stabilità del token.

Quando un utente acquista una stablecoin, l'emittente riceve valuta fiat che viene conservata nelle riserve. In cambio, vengono emessi nuovi token che entrano in circolazione. Al momento del riscatto, i token vengono *bruciati*, ovvero eliminati dalla circolazione, e l'equivalente in valuta fiat viene rilasciato dalle riserve all'utente.

La Figura 3.1 rappresenta il ciclo di vita operativo di una stablecoin collateralizzata con fiat, e mostra il processo di creazione e gestione delle riserve che permette alla stablecoin di mantenere il **peg** con l'asset di riferimento.

Il peg si riferisce al legame o all'ancoraggio del valore della stablecoin a un'altra valuta o asset, solitamente una valuta fiat, come il dollaro USA. Questo peg è mantenuto grazie alla gestione delle riserve in valuta fiat o in asset equivalenti, piuttosto che tramite uno smart contract, come avviene per altre tipologie di stablecoin, ad esempio stablecoin algoritmiche o cripto-collateralizzate (Sezioni 3.1.2 e 3.1.3). Quando un utente invia valuta fiat all'emittente della stablecoin (passo 1), quest'ultima deposita i fondi presso una banca (passo 2). Le riserve di USD vengono gestite per garantire liquidità a breve termine (passo 3a), mentre una parte può essere investite in asset sicuri a breve termine (passo 3b). Una volta confermata la riserva, l'emittente fornisce all'utente una quantità equivalente di stablecoin (passo 4), che può essere custodita in un wallet centralizzato o trasferita a un wallet compatibile con la blockchain (passo 5). Questo processo sottolinea l'importanza della trasparenza e della gestione delle riserve per garantire la stabilità delle stablecoin collateralizzate con fiat, elemento cruciale per la loro credibilità sul mercato.

[1]La moneta fiat è una valuta nazionale non ancorata al prezzo di una materia prima come oro o argento. Il valore di una moneta fiat è legato in larga parte alla fiducia nei confronti dell'autorità che la emette, di norma uno Stato o una banca centrale [22].

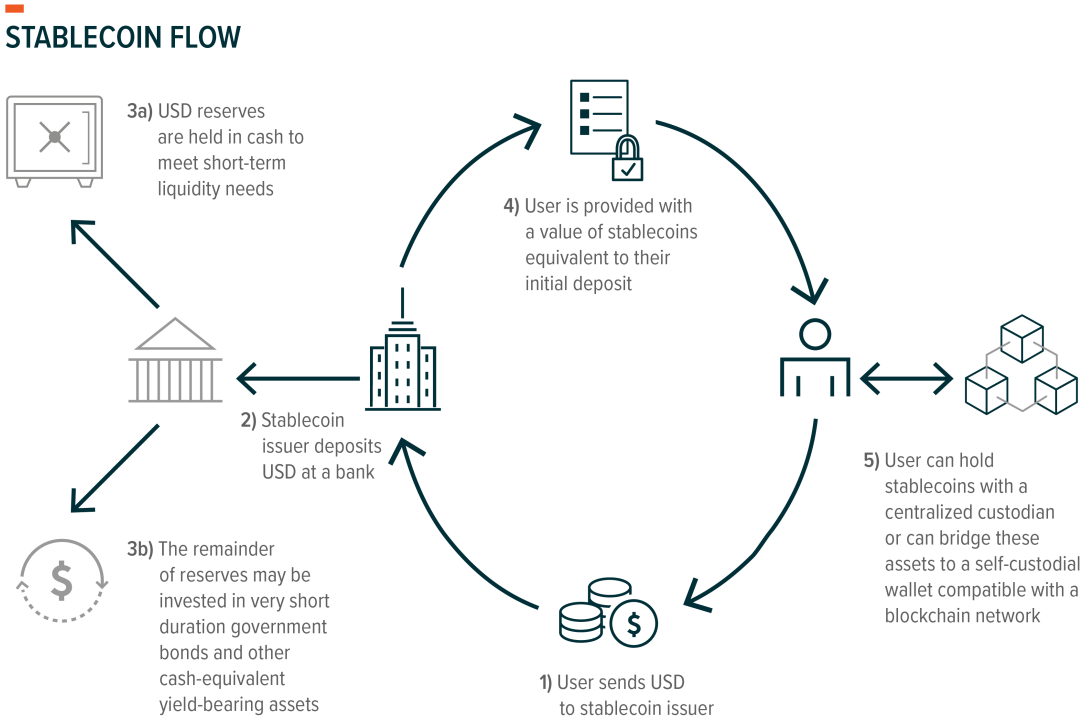


Figura 3.1: Flusso operativo delle stablecoin collateralizzate con fiat [23]

3.1.2 Stablecoin collateralizzate con criptovalute

Le stablecoin collateralizzate con criptovalute rappresentano un'alternativa decentralizzata a quelle garantite da riserve di valuta fiat. Queste stablecoin operano in modo completamente decentralizzato grazie all'uso di smart contract sulla blockchain dove garantiscono trasparenza, automazione e indipendenza da intermediari centralizzati.

Il valore della stablecoin è ottenuto tramite meccanismi di *sovra-collateralizzazione* [24]. Gli utenti che desiderano emettere stablecoin devono depositare una quantità di criptovaluta che eccede il valore delle stablecoin emesse, solitamente con un rapporto di collateralizzazione superiore al 100%. Ad esempio, per generare 100 unità di una stablecoin, potrebbe essere richiesto un collaterale pari a 150 dollari in criptovalute. Questo margine protegge il sistema da fluttuazioni di prezzo tipiche delle criptovalute utilizzate come collaterale. Il mantenimento della stabilità è inoltre supportato da un sistema di *liquidazione automatica*, in cui gli smart contract vendono il collaterale degli utenti quando il suo valore scende al di sotto di una soglia critica. Questo processo è essenziale per garantire che il valore della stablecoin non perda il legame con l'asset di riferimento. Tali liquidazioni

sono regolate da parametri specifici, come il *rapporto di liquidazione*, che definisce il livello minimo di collateralizzazione richiesto per mantenere sicurezza del sistema [25]

Tuttavia queste stablecoin presentano alcuni svantaggi come la necessità di sovra-collateralizzazione che comporta un'inefficienza nell'uso capitale, poiché un parte significativa delle risorse deve rimanere bloccata come garanzia. Inoltre, durante periodi di estrema volatilità del mercato, gli utenti possono subire liquidazioni forzate che potrebbero portare a perdite. Tuttavia, l'approccio decentralizzato e l'assenza di intermediari centralizzati rendono queste stablecoin un pilastro fondamentale della DeFi, garantendo stabilità attraverso un sistema interamente programmabile e gestito tramite blockchain.

3.1.3 Stablecoin algoritmiche

Le stablecoin algoritmiche sono state progettate per mantenere un valore stabile senza l'uso di collaterali fisici, come riserve di valuta fiat o criptovalute. A differenza delle stablecoin collateralizzate, queste monete si basano esclusivamente su algoritmi e meccanismi automatici per regolare dinamicamente l'offerta del token in base alla domanda di mercato. L'asset di riferimento, ossia il valore target che queste stablecoin cercano di mantenere, è tipicamente una valuta fiat come il dollaro statunitense. Tuttavia, a differenza delle stablecoin fiat-collateralizzate, non esistono riserve reali di dollari a sostegno della stablecoin: la stabilità è ottenuta tramite meccanismi programmati che agiscono direttamente sull'offerta. Questo approccio si fonda sull'idea che modificando l'offerta del token in base alle variazioni di domanda sia possibile mantenere il valore della stablecoin vicino all'asset di riferimento. Ad esempio, quando il prezzo della stablecoin supera il valore target (ad esempio 1 USD), l'algoritmo aumenta l'offerta generando nuovi token per abbassare il prezzo. Al contrario, quando il prezzo scende sotto il valore target, l'algoritmo riduce l'offerta, "bruciando" token per aumentarne la scarsità e riportare il valore in linea con il target.

Nonostante l'innovazione del modello, le stablecoin algoritmiche presentano vulnerabilità significative. La mancanza di un collaterale reale le rende fortemente dipendenti dal comportamento degli utenti che partecipano al sistema. Questo modello presuppone che le persone agiscano in modo da mantenere il valore della stablecoin da mantenere il valore della stablecoin vicino al target, ad esempio comprandola quando il prezzo è basso e vendendola quando è alto. Tuttavia in momenti di forte instabilità o perdita di fiducia, queste ipotesi possono venire meno, portando a rapidi crolli. È quanto accaduto nel caso di TerraUSD [26], in cui il valore della stablecoin è precipitato a causa di una perdita di fiducia, scatenando una reazione a catena che ha causato il crollo dell'intero ecosistema collegato; verrà approfondito nella Sezione 3.4.

3.2 Ruolo delle stablecoin nel mercato DeFi

Le stablecoin hanno assunto un ruolo centrale nell'ecosistema della *finanza decentralizzata (DeFi)* e nei sistemi finanziari basati su blockchain. DeFi è un termine generale che si usa per indicare i servizi finanziari eseguiti su blockchain pubbliche, principalmente sulla blockchain di Ethereum. In molti di questi protocolli le stablecoin sono utilizzate come unità di misura per i prezzi di altri asset.

Le stablecoin facilitano gli scambi tra criptovalute su piattaforme *DEX*[2] come *Uniswap* o *SushiSwap* [27], fornendo una base stabile per le coppie di trading. Ad esempio, invece di scambiare direttamente Bitcoin con Ether, un utente potrebbe vendere Bitcoin per USDC o DAI, e successivamente acquistare Ether utilizzando quella stablecoin. Questo approccio minimizza il rischio associato alla volatilità dei prezzi tra le due criptovalute durante l'esecuzione della transazione.

Le stablecoin sono molto importanti per i *pool di liquidità*, in cui gli utenti forniscono asset in coppie per facilitare gli scambi. Essendo meno volatili, stabilizzano il valore dei pool e offrono un'opzione sicura per gli utenti che vogliono contribuire con asset più stabili.

3.2.1 Stablecoin nei protocolli di lending/borrowing

Questi protocolli utilizzano le stablecoin per permettere agli utenti di ottenere prestiti in un ambiente decentralizzato e privo di intermediari. Depositando collaterale, gli utenti possono accedere a liquidità immediata senza dover vendere i propri asset, evitando così di subire perdite in caso di aumento del valore delle criptovalute depositate. Tuttavia, la volatilità del collaterale può innescare la liquidazione automatica del prestito qualora il suo valore scenda sotto la soglia necessaria per coprirlo [28]. Ad esempio, se un utente ha preso in prestito DAI e il valore del collaterale in ETH cala bruscamente, il sistema potrebbe liquidare il prestito.

Un'altra attività molto popolare è il *yield farming* che consiste nel collocare asset di criptovaluta in un pool di liquidità o in un'altra piattaforma di finanza decentralizzata (DeFi) per ottenere un rendimento più elevato. Tuttavia ci sono diversi rischi associati allo yield farming e all'uso di stablecoin nei protocolli DeFi. Oltre alla *perdita temporanea* causata dalle oscillazioni di prezzo tra gli asset depositati nei pool di liquidità, ci sono rischi legati ai *bug negli smart contract* o a *possibili hack*, che possono rendere i fondi vulnerabili a furti. Un altro rischio comune è il *rug pull*, ovvero una truffa in cui i fondatori di un progetto abbandonano improvvisamente la piattaforma, sottraendo tutta la liquidità fornita dagli investitori. La volatilità del mercato rappresenta anch'essa un fattore critico, poiché criptovalute possono subire

[2]DEX, exchange decentralizzato, è un mercato peer-to-peer in cui le transazioni avvengono direttamente tra gli operatori di criptovalute. Favoriscono le transazioni finanziarie che non sono officiate da banche, broker o altri intermediari.

cali di valore durante il periodo di staking, esponendo l'utente a perdite maggiori di quelle guadagnate attraverso i rendimenti [29].

3.3 Stablecoin e token scelti per l'analisi

Ethereum è la blockchain più utilizzata per l'emissione e la gestione di token, con lo standard ERC-20 come protocollo di riferimento per la creazione di asset digitali. Nel vasto ecosistema di token Ethereum, alcuni emergono per la loro rilevanza economica e operativa. Ci interessava analizzare le principali stablecoin e abbiamo cercato quali erano le principali in termini di trasferimenti. Secondo i dati riportati in Tabella 3.1 tra i primi quattro contratti ERC-20, tre sono stablecoin, mentre Wrapped Ether (WETH) rappresenta un caso particolare di "*quasi-stablecoin collateralizzata con criptovalute*" [30]. Inoltre la capitalizzazione di mercato di questi token è molto rilevante superando di gran lunga l'ordine dei milioni di USD.

Contract address	Token name	N. of Transfers	Percentage	Market Cap.
dac17f958d2ee523a2206206994597c13d831ec7	Tether USD (USDT)	149 408 698	15.537	67 Mld
c02aaa39b223fe8d0a0e5c4f27ead9083c756cc2	Wrapped Ether (WETH)	104 183 120	10.834	9 Mld
a0b86991c6218b36c1d19d4a2e9eb0ce3606eb48	USD Coin (USDC)	42 601 224	4.430	56 Mld
6b175474e89094c44da98b954eedeac495271d0f	Dai Stablecoin (DAI)	14 387 573	1.496	6.3 Mld
514910771af9ca656af840dff83e8264ecf986ca	ChainLink Token (LINK)	11 388 177	1.184	3.2 Mld
174bfa6600bf90c885c7c01c7031389ed1461ab9	More Gold Coin (MGC)	8 947 669	0.930	2.86 Mld
95ad61b0a150d79219dcf64e1e6cc01f0b64c4ce	SHIBA INU (SHIB)	7 781 424	0.809	6.2 Mld
990f341946a3fdb507ae7e52d17851b87168017c	Strong (STRONG)	6 964 935	0.724	3.2 Mld
58b6a8a33023c9daeac383334672404ee733ab239	Livepeer Token (LPT)	6 025 932	0.627	222 Mln
03cb0021808442ad5efb61197966aef72a1def96	coToken (coToken)	5 370 855	0.559	89 Mln
Total		**357 059 607**	**37.130**	**148.7 Mld**

Tabella 3.1: Confronto tra i principali token per numero di trasferimenti e percentuale [31].

I quattro token di analisi si classificano in diverse categorie di stablecoin. In particolare Tether (USDT) e USD Coin (USDC) sono stablecoin collateralizzate fiat mentre DAI Stablecoin (DAI) è collateralizzata con criptovalute. WETH è un token "wrappato" che permette di utilizzare la criptovaluta di Ethereum nativa ETH sullo standard ERC-20 "wrappandola" come token fungibile. Questo processo viene descritto approfonditamente nella Sezione 3.3.4).

Di seguito fornisco un'analisi approfondita di ogni token scelto per l'analisi e un bonus su una stablecoin algoritmica (TerraUSD) per mostrare la sua sensibilità.

3.3.1 Tether

Tether (USDT), introdotta nel 2014, è una stablecoin centralizzata ancorata al dollaro statunitense che ha trasformato l'ecosistema delle criptovalute offrendo una

soluzione stabile alla volatilità tipica di asset come BTC ed ETH. USDT, acronimo di *Tether USD*, è il nome del token emesso da Tether Limited per rappresentare il valore della stablecoin. Il suo valore è mantenuto grazie alla collateralizzazione in valuta fiat. Come spiega il white paper originale di Tether [32]:

> *Ogni unità di Tether emessa in circolazione è garantita con un rapporto 1:1 (ovvero, un USDT vale un dollaro statunitense) dalla corrispondente unità di valuta fiat nelle riserve della società Tether Limited con sede a Hong Kong.*

Quando un utente invia USD all'emittente di Tether, riceve una quantità equivalente di USDT, che può utilizzare nelle transazioni su blockchain compatibili. Gli utenti possono successivamente riconvertire i loro USDT in USD, facendo sì che l'emittente distrugga i token restituiti.

Sebbene Tether sia stata introdotta nel 2014, inizialmente era implementata sulla blockchain di Bitcoin tramite il protocollo Omni Layer. Solo successivamente, con l'introduzione di Ethereum nel 2015, Tether ha ampliato il supporto alla blockchain Ethereum e ad altre reti, come Tron e Binance Smart Chain [33].

Trasparenze, controversie e fattori di successo

Tether ha affrontato numerose controversie legate alla trasparenza delle sue riserve. Infatti l'azienda per anni è stata criticata per la mancata pubblicazione di audit completi che confermassero l'esistenza delle riserve dichiarate. In risposta alle critiche, Tether ha iniziato a pubblicare report finanziari periodici che mostravano il possesso delle riserve [34]. Tuttavia, molte di queste riserve non sono necessariamente detenute in contanti, ma includono anche altri strumenti finanziari, il che ha sollevato ulteriori dubbi sulla liquidità immediata di Tether in caso di grandi richieste di ritiro simultaneo.

Tether ha consolidato la sua posizione di leader tra le stablecoin grazie ad una combinazione di fattori interni ed esterni. Essendo stata una delle prime stablecoin sul mercato, USDT ha beneficiato di una rapida adozione sia da parte degli exchange che degli utenti. Inoltre ha implementato una riserva per mantenere il peg con asset con alta liquidità, come titoli di stato e depositi bancari ed è *multi-chain*, ovvero indica che può essere emessa e utilizzata su diverse blockchain.

3.3.2 USD Coin

USD Coin (USDC) è una stablecoin collateralizzata con fiat, ancorata al valore del dollaro statunitense con un rapporto 1:1. Lanciata nel 2018 da *Circle* in collaborazione con *Coinbase* [35], USDC si è rapidamente affermata come una delle principali stablecoin sul mercato.

USDC viene emessa su diverse blockchain: in Ethereum l'emissione avviene sotto forma di token ERC-20, mentre su altre piattaforme sono adottati standard equivalenti. Ad esempio, viene emesso come token *BEP-20* sulla blockchain di *Binance Smart Chain* [36] e come *SPL* token sulla blockchain di *Solana* [37]. Ogni USDC emesso è garantito da riserve di dollari statunitensi detenuti in conti bancari controllati e supervisionati. Inoltre, in confronto con Tether, le riserve sono soggette a verifiche e audit mensili condotti da società indipendenti, il che offre una maggiore trasparenza. Il modello di funzionamento di USDC prevede che quando un utente deposita USD su un account gestito da Circle, una quantità equivalente di USDC viene emessa e inviata all'utente. Successivamente quando l'utente desidera convertire i suoi USDC in USD, i token vengono bruciati e il denaro fiat viene restituito. Si tratta dunque di un meccanismo molto simile a quello di Tether che garantisce che ci sia sempre una riserva sufficiente per coprire l'intero ammontare di USDC in circolazione.

Circle è conforme alle normative del *FinCEN (Financial Crimes Enforcement NEtwork)* [38] degli Stati Uniti, e le riserve di USDC sono regolarmente verificate da revisori terzi. Questa trasparenza e aderenza alle leggi rende USDC una delle stablecoin più affidabili e regolamentate sul mercato. Inoltre Circle è costantemente impegnata a promuovere standard più elevati di trasparenza finanziaria, pubblicando mensilmente i rapporti che certificano le riserve di USD che garantiscono i token USDC [39].

USDC è utilizzata in attività di trading, nella finanza decentralizzata (DeFi) come *Uniswap* e nei pagamenti. Per quanto riguarda i pagamenti, Circle ha sviluppato partnership con varie piattaforme di pagamento per utilizzare USDC nelle transazioni globali, eliminando la necessità di intermediari e riducendo i costi associati ai trasferimenti transfrontalieri.

3.3.3 DAI

DAI è una stablecoin *collateralizzata da criptovalute* (Sezione 3.1.2) e gestita tramite un sistema completamente decentralizzato, sviluppato dalla piattaforma *MakerDAO*. Il suo valore è ancorato al dollaro statunitense e mantenuto attraverso meccanismi decentralizzati di sovra-collateralizzazione e gestione del rischio automatizzata. DAI non è supportata da riserve di dollari o altre asset fiat, ma utilizza esclusivamente *collaterale in criptovalute*, rendendo il suo funzionamento completamente decentralizzato.

Come discusso nella Sezione 3.1.2, il valore di DAI è mantenuto stabile attraverso un sistema di smart contract operante su MakerDAO. Gli utenti che desiderano generare DAI devono depositare criptovalute, come ETH, in un *Maker Vault*, uno smart contract che consente di bloccare tali asset come collaterale per emettere DAI. Per garantire la sicurezza del sistema, è richiesto un rapporto di collateralizzazione

di almeno il 150%: ad esempio, per emettere 100 DAI (equivalenti a 100 USD), l'utente deve depositare criptovalute per un valore minimo di 150 USD. Questo margine protegge il sistema da fluttuazioni nel valore del collaterale [40].

Uno degli elementi più potenti di DAI è la *governance decentralizzata* gestita tramite il protocollo MakerDAO, attraverso il token *MKR*[3]. I possessori di MKR hanno il diritto di voto su importanti decisioni, come l'aggiunta di nuovi asset come collaterale, la modifica di parametri del sistema e l'evoluzione futura del protocollo, garantendo che nessuna entità centrale possa controllare DAI o manipolare il funzionamento [25].

3.3.4 Wrapped Ether

Wrapped Ether (WETH) è una versione tokenizzata di ETH progettata per essere compatibile con lo standard ERC-20. Questa caratteristica è fondamentale per garantire l'interoperabilità con i protocolli DeFi e gli smart contract su Ethereum, dato che il formato nativo di ETH non soddisfa i requisiti tecnici dello standard ERC-20. Il "wrapping" consente quindi a ETH di partecipare in modo efficace nelle operazioni DeFi, come il trading, il prestito e il pool di liquidità. Gli utenti inviano ETH a uno smart contract dedicato, che blocca l'ETH ricevuto e rilascia un numero equivalente di WETH. I fondi bloccati rimangono nello smart contract fino a quando l'utente decide di "unwrappare" il proprio WETH, recuperando l'ETH originariamente inviato. Durante il processo di unwrapping, i token WETH restituiti vengono automaticamente bruciati, garantendo che il valore totale in circolazione rimanga sempre coperto dall'ETH nel contratto. Questa dinamica rende il sistema completamente trasparente e verificabile, poiché chiunque può controllare lo smart contract per confermare la quantità di ETH custodita e la corrispondente quantità di WETH emesse.

WETH può anche essere impiegato come collaterale in protocolli lending/borrowing come *Aave*[4] e *Compound*[5], partecipando anche ad attività di yield farming. Un'altra caratteristica importante è che, essendo un token ERC-20, WETH può essere trasferito su altre blockchain compatibili con ERC-20, aumentando la sua versatilità e consentendo una maggiore interoperabilità tra reti diverse. Tuttavia, è importante notare che la versione di WETH utilizzata su altre blockchain potrebbe avere un meccanismo di wrapping diverso, gestito da protocolli specifici [30]. L'uni-

[3]MKR è il token governance del protocollo MakerDAO, utilizzato per prendere decisioni importanti all'interno del sistema.

[4]Aave è un protocollo decentralizzato che consente agli utenti di depositare asset come collaterale per prendere in prestito altre criptovalute.

[5]Compound è una piattaforma DeFi che permette agli utenti di guadagnare interessi prestando le proprie criptovalute o di prendere in prestito altri asset in cambio di collaterali.

co svantaggio è che, essendo un token, WETH non può essere utilizzato per pagare le *gas* su Ethereum, una funzione riservata esclusivamente a ETH.

3.4 TerraUSD: Una stablecoin algoritmica

Nonostante *TerraUSD* (*USTC)* non sia inclusa nelle analisi sperimentali di questa tesi, la sua storia e il crollo significativo che ha subito nel 2022 rappresentano un evento cruciale nella storia delle stablecoin.

TerraUSD, precedentemente *UST*, è stata una stablecoin algoritmica creata per essere una valuta stabile ancorata al dollaro USA e progettata per essere usata nel vasto ecosistema di applicazioni di Terra blockchain [41]. L'acronimo *UST* è il ticker tra Terra (la blockchain dove è nata la stablecoin) e l'acronimo del dollaro statunitense, USD. La stablecoin quindi non era collateralizzata da riserve in dollari o asset tradizionali ma basava la sua stabilità su un algoritmo che gestiva l'interazione tra UST e il token nativo *LUNA*[6].

Il meccanismo di peg di UST si basava sull'arbitraggio: nel caso in cui il prezzo fosse sceso al di sotto di 1$, gli utenti avrebbero potuto acquistare UST a un prezzo inferiore e convertirlo in 1$ di LUNA. Questa operazione avrebbe bruciato UST e ridotto di conseguenza l'offerta, provocando un aumento del prezzo. Al contrario, nel caso in cui UST avesse superato 1$, gli utenti avrebbero potuto convertire LUNA in UST, aumentando l'offerta, con conseguente diminuzione del prezzo.

3.4.1 Il crollo

Nel maggio 2022, il crollo di TerraUSD ha scosso il mercato delle criptovalute. L'evento ha avuto origine quando il protocollo *Anchor*[7] ha iniziato a mostrare segni di insostenibilità. Esso offriva ai depositatari di UST rendimenti elevati, fino al 20% all'anno, un tasso estremamente attraente rispetto ad altre stablecoin come USDT e USDC. Questo ha comportato un eccessivo afflusso di depositi, ma il sistema Terra non era in grado di sostenere tali rendimenti a lungo termine [42]. Il 7 maggio 2022, due grandi indirizzi hanno ritirato 375 milioni di UST da Anchor, scatenando una serie di vendite che ha portato il prezzo di UST a scendere al di sotto del peg di 1$. Nonostante gli sforzi di TerraForm Labs per stabilizzare il peg, la crisi si è intensificata. In soli tre giorni, il valore di UST è crollato, raggiungendo 0.75$, e anche LUNA ha visto un drastico calo del suo valore, creando una situazione di

[6]LUNA era un token nativo della blockchain Terra e svolgeva un ruolo centrale nel meccanismo di stabilizzazione. Attraverso il meccanismo *mint and burn* LUNA veniva bruciato per emettere UST e viceversa per il riscatto.

[7]Anchor Protocol è un servizio di lending che nasce per offrire prestiti e interessi su stablecoin nella blockchain Terra.

panico collettivo nel mercato. Questo spiega la fragilità delle stablecoin algoritmiche data la mancanza di un collaterale. Dato che una stablecoin algoritmica è molto dipendente dal comportamento degli utenti che partecipano al sistema, la vendita dei due grandi indirizzi di UST ha scatenato un evento a catena, portando UST al collasso.

Quando il valore di LUNA è crollato, molti investitori sono stati indotti a vendere le proprie riserve di UST, determinando dunque un crollo del prezzo della stablecoin. Secondo lo studio pubblicato dal *National Bureau of Economic Research (NBER)* [42], il crollo non sembra essere stato il risultato di una manipolazione di mercato concentrata, ma piuttosto la *conseguenza* di preoccupazioni crescenti sulla sostenibilità del sistema di Terra. Il comportamento degli investitori durante la crisi ha anche messo in luce una disuguaglianza informativa tra gli attori del mercato, con più esperti che sono riusciti a mitigare le perdite mentre i meno informati hanno subito danni più gravi.

3.5 Conclusioni

Il caso di TerraUSD ha sottolineato i limiti delle stablecoin algoritmiche e le sfide legate alla loro sostenibilità. Il principale problema è legato al rischio di disallineamento tra domanda e offerta nei momenti di stress di mercato, dove la fiducia degli investitori può crollare rapidamente. Questo ha aperto una riflessione più ampia sull'affidabilità delle stablecoin e sulla necessità di meccanismi di garanzia più solidi, come quelli offerti dalle stablecoin collateralizzate, che sembrano meglio attrezzate per affrontare la volatilità e mantenere l'ancoraggio anche in condizioni di mercato avverse. Sebbene le stablecoin collateralizzate con fiat come USDT e USDC siano considerate più sicure grazie alla loro parità con il dollaro e al supporto di riserve reali, restano delle preoccupazioni circa la trasparenza delle riserve e la loro gestione centralizzata, come evidenziato nelle Sezioni 3.3.1 e 3.3.2.

È importante notare come le stablecoin ERC-20, pur presentando sfide, abbiano un ruolo centrale all'interno della DeFi. I capitoli successivi esploreranno appunto l'*analisi delle transazioni ERC-20* per queste stablecoin trattate.

Capitolo 4

Struttura dei grafi per ERC-20

Le transazioni ERC-20 tra utenti possono essere viste come flussi di valore economico che vengono registrati mediante la blockchain. Per comprendere meglio come queste transazioni si sviluppano nel tempo e come gli attori principali si comportano, risulta spesso utile modellare queste interazioni tramite grafi, strutture matematiche utilizzata per rappresentare insiemi di oggetti e le relazioni tra di essi. Questo approccio permette di ottenere una visione strutturale e dinamica delle relazioni economiche tra i partecipanti, facilitando l'identificazione di nodi centrali, pattern ricorrenti e dinamiche evolutive all'interno delle reti.

Questo capitolo è dedicato alla modellazione delle reti di transazioni ERC-20 tramite *grafi diretti e pesati*. In particolare, ogni nodo nel grafo rappresenta un indirizzo Ethereum utilizzato in un contratto ERC-20, mentre gli archi tra i nodi rappresentano le transazioni che avvengono tra due indirizzi. Come sarà illustrato nel corso del capitolo, ogni arco può essere associato a diversi pesi in base alle proprietà delle transazioni che si desidera studiare, come ad esempio il timestamp dello scambio o la quantità di token trasferiti fra i due utenti.

4.1 Rappresentazione tramite grafi

La rappresentazione mediante grafi dei dati transazionali è uno strumento chiave per analizzare le complesse interazioni che emergono all'interno dell'ecosistema di Ethereum [43]. Nel corso della tesi utilizziamo questo tipo di rappresentazione per studiare le transazioni riguardanti i trasferimenti di token ERC-20, concentrandoci in particolare sulle economie associate alle stablecoin USDT, USDC, DAI e WETH. Più precisamente, gli scambi di token ERC-20 sono rappresentati mediante grafi *orientati* in cui i nodi (o vertici) rappresentano gli indirizzi dei wallet o degli smart contract, mentre gli archi (o collegamenti) rappresentano le transazioni tra di essi. Trattandosi di grafi orientati, ogni arco indica la direzione del trasferimento di token

da un mittente a un destinatario. Questa proprietà del modello di rappresentazione consente di mantenere informazioni importanti non solo sulle interazioni, ma anche sulla direzione dei flussi economici.

Per ciascuna delle economie associate alle stablecoin che saranno analizzate in questa tesi, si è scelto di costruire due diverse tipologie di grafi di trasferimenti. Tale scelta è motivata dalla volontà di ottenere sia una visione più globale di tali economie, sia una visione più dettagliata e capace di riflettere maggiormente l'evoluzione degli scambi nel corso del tempo. Più precisamente, per ciascuno dei quattro token studiati sono stati definiti:

1. un **grafo globale** in grado di catturare la totalità dei trasferimenti della stablecoin presenti nel dataset di riferimento;

2. una serie di grafi che rappresentano i trasferimenti contenuti in **chunk temporali**. Per la precisione, ogni singolo chunk temporale è costituito da una sequenza di trasferimenti consecutivi effettuati nell'arco di un periodo di tempo prefissato. Si noti che per l'analisi sono stati utilizzati chunk aventi ampiezza pari a 4 settimane, quindi un mese.

4.2 Modellazione del grafo globale

Il grafo globale fornisce una visione completa delle transazioni ERC-20 effettuate per ciascuna stablecoin, consentendo di catturare l'intera gamma di interazioni economiche all'interno della blockchain di Ethereum. Poiché fra due indirizzi vi possono essere molteplici trasferimenti di token ERC-20, si è scelto di modellare il grafo globale mediante un *multigrafo diretto*, ammettendo dunque la possibilità di avere più di un arco orientato fra due nodi.

Struttura del grafo

Nel multigrafo diretto ogni transazione tra due nodi è rappresentata da un arco distinto, mantenendo la direzione del trasferimento. Per catturare l'informazione associata a ciascun trasferimento, inoltre, ogni arco contiene due pesi:

- **Valore economico della transazione**: Rappresenta la quantità di stablecoin trasferita tra mittente e destinatario.

- **Timestamp della transazione**: Indica il momento preciso in cui è avvenuta la transazione sulla blockchain.

Questi due pesi forniscono informazioni sia economiche che temporali, permettendo di monitorare l'andamento delle transazioni nel tempo e di quantificare i volumi di token trasferiti tra i vari wallet.

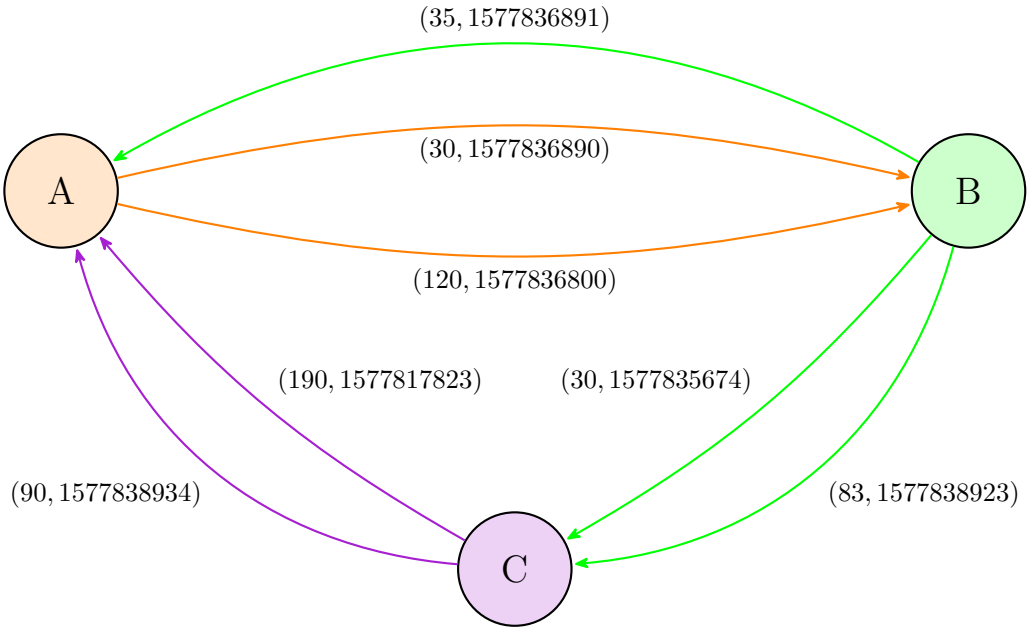


Figura 4.1: Esempio della struttura del multi-grafo globale ponderato

La Figura 4.1 rappresenta un esempio di come è modellato il multigrafo ponderato globale per ogni stablecoin. Come si può notare ci sono multiarchi tra i diversi nodi ognuno con informazioni diverse. Ad esempio dal nodo A verso il nodo B partono due archi (transazioni) diversi rispettivamente con valore uguale a 30 e 120 e timestamp diverso; dal nodo B partono due transazioni con pesi rispettivamente 30 e 83, per il valore trasferito, e timestamp 1577835674 e 1577838923; e così via.

Motivazioni per la scelta del grafo globale

La scelta di rappresentare le reti di stablecoin tramite un multi-grafo diretto e pesato è guidata dall'obiettivo di catturare tutta la complessità delle transazioni senza semplificarla. La blockchain di Ethereum è un sistema complesso (Sezione 2.2), in cui le transazioni avvengono continuamente tra milioni di wallet. Utilizzare questa rappresentazione consente di preservare ogni singola transazione, rispettando la direzione del flusso economico.

Includere i timestamp come uno dei pesi sugli archi offre la possibilità di monitorare la dinamicità delle transazioni. Il grafo globale rappresenta una base solida per calcolare misure di centralità, come il **Pagerank** [44], algoritmo utilizzato per misurare l'influenza o l'importanza relativa di un nodo all'interno del grafo delle transazioni dove calcola la probabilità che un nodo venga raggiunto tramite le transazioni di token attraverso un indice assegnato ad ognuno di essi (Sezione 5.9).

Infine, il grafo globale fornisce una base strutturale da cui partire per confrontare la rete con le versioni suddivise in chunk temporali. Avere un modello completo di tutte le transazioni offre un punto di riferimento per comprendere le variazioni che emergono quando la rete viene esaminata in periodi di tempo più brevi. In questo modo, è possibile identificare le differenze comportamentali tra il grafo complessivo e le sue versioni temporali, evidenziando come i ruoli economici dei nodi e la struttura della rete si adattino nel tempo.

4.2.1 Grafo collassato

Per alcune statistiche abbiamo avuto bisogno di collassare il grafo globale come faremo nei chunk temporali (Sezione 4.3). In particolare le transazioni multiple tra gli stessi nodi (multiarchi) vengono collassate in un *unico arco diretto* per ridurre complessità, mantenendo però due pesi distinti per catturare le informazioni essenziali sulle interazioni tra i nodi:

- **Molteplicità**: Il primo peso rappresenta la molteplicità, ovvero il numero totale di transazioni tra due nodi in quel periodo. Ad esempio, se tra i nodi A e B sono avvenute 5 transazioni nel mese di gennaio, l'arco diretto $A \to B$ avrà un peso che rappresenta il conteggio delle transazioni (peso1 = 5) aggregato a quell'arco.

- **Somma dei valori**: Il secondo peso rappresenta la somma dei valori delle transazioni tra due nodi nel periodo considerato. Se nelle 5 transazioni tra A e B sono stati trasferiti rispettivamente 10, 20, 15, 5 e 30 unità di stablecoin, il peso aggregato (peso2) sarà pari a 80. Questo peso riflette il valore economico complessivo delle transazioni tra i due nodi.

L'aggregazione delle transazioni in un unico arco riduce notevolmente la complessità del grafo, soprattutto in reti molto attive, senza perdere informazioni rilevanti.

Queste statistiche comprendono il PageRank e altri score come Hub Score e Authority Score, che sono misure di centralità critiche per analizzare e comprendere a pieno quali nodi sono più attivi o "importanti" nella rete stessa. Questo perché in primo luogo l'algoritmo utilizzato per il calcolo del PageRank non supporta i multigrafi, ovvero non ne tiene conto, mentre per il calcolo degli altri score possiamo studiare due centralità differenti basate sul numero di trasferimenti tra due nodi e la somma dei valori trasferiti tra due nodi, e quindi 2 pesi differenti nel grafo. Tutto ciò verrà approfondito nella Sezione 5.9.

Per comprendere meglio come il grafo viene creato, vediamo un piccolo esempio di modellazione del grafo collassato:

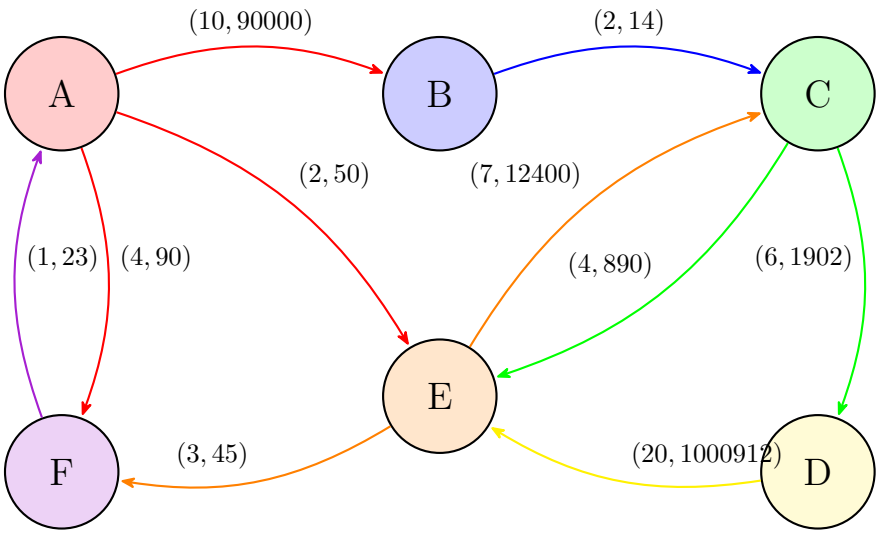


Figura 4.2: Esempio della struttura del grafo collassato ponderato per ogni chunk mensile

Come mostrato in Figura 4.2, gli archi sono stati consolidati, garantendo che ogni nodo abbia al più un arco verso ciascun altro nodo. Ad esempio, il nodo A presenta tre archi uscenti, uno per ciascuno degli altri nodi B, E ed F. È importante notare che, essendo un grafo diretto, la presenza di un arco tra due nodi non implica necessariamente una connessione bidirezionale. Un esempio significativo è rappresentato dagli archi tra A e B: A ha un arco diretto verso B, indicando che sono avvenute transazioni da A a B, ma non vi è alcun arco da B a A, il che significa che non ci sono state transazioni da B verso A in questo specifico intervallo temporale.

Come possiamo notare i pesi qui cambiano, infatti vediamo come primo peso la molteplicità e il secondo la somma complessiva dei valori trasferiti. Ad esempio A ha effettuato 10 transazioni verso B con somma totale di 90000 token.

4.3 Modellazione dei chunk temporali

La suddivisione temporale delle transazioni ERC-20 in chunk mensili rappresenta un passaggio fondamentale per catturare le dinamiche evolutive delle reti di stablecoin. Mentre il grafo globale fornisce una visione complessiva delle transazioni, la suddivisione in chunk permette di osservare come queste interazioni cambiano e si sviluppano in periodi di tempo definiti. Questo approccio consente di identificare trend mensili, pattern ricorrenti o anomalie, e di analizzare come si evolvono i ruoli degli attori principali in risposta a fattori esterni come eventi di mercato o fluttuazioni di domanda.

Per ogni chunk temporale è stato costruito un grafo collassato, diretto e pesato, come per il grafo globale, spiegata nella Sezione 4.2.1

Motivazione per la suddivisione temporale

Le reti economiche non sono statiche, ma subiscono continui cambiamenti, spesso dovuti a dinamiche di mercato o innovazioni tecnologiche [45]. La suddivisione temporale permette di identificare queste variazioni e analizzare come la rete reagisce a specifici eventi, come fluttuazioni di mercato o cambiamenti nell'adozione della stablecoin [46]. Ogni chunk temporale viene quindi confrontato con i precedenti per osservare cambiamenti strutturali e comportamentali all'interno della rete. Questo confronto consente di capire come i nodi più centrali e le connessioni tra i partecipanti si evolvono nel tempo.

Un beneficio fondamentale della suddivisione temporale è la possibilità di monitorare l'evoluzione dinamica della centralità dei nodi all'interno della rete. Nei grafi globali, la centralità di un nodo offre un'istantanea complessiva della sua importanza all'interno della rete nel corso di tutto il periodo di osservazione. Tuttavia, non permette di catturare come questa centralità possa cambiare nel tempo, a seconda delle condizioni del mercato, della domanda di stablecoin o fasi di alta volatilità del mercato [47]. Questo fenomeno è correlato alla stabilità delle misure di centralità, come sottolineato da [48], che evidenzia come alcune misure di centralità rimangano stabili nel tempo, mentre altre possono variare drasticamente in risposta a perturbazioni del grafo e quindi condizionare gli attori della rete a prendere decisioni rapide e importanti, come nel caso di TerraUSD (Sezione 3.4).

La modellazione dei chunk temporali, supportata dall'uso di grafi diretti e pesati, fornisce una rappresentazione dinamica e dettagliata delle reti di stablecoin. Questa metodologia consente di comprendere non solo le caratteristiche statiche della rete, ma anche come i nodi e le loro interazioni evolvono nel tempo, fornendo insight cruciali per l'analisi dei comportamenti economici.

4.4 Librerie utilizzate

Nella fase di modellazione e analisi delle reti di transazioni ERC-20, l'utilizzo di strumenti efficienti e scalabili è stato cruciale per gestire l'enorme quantità di dati provenienti dalla blockchain di Ethereum. Per rappresentare, analizzare e interpretare queste complesse reti, sono state adottate due librerie principali: *Igraph* sviluppata in C++ e *Webgraph* in Java.

Entrambe le librerie sono state selezionate per le loro caratteristiche specifiche: Igraph eccelle nel fornire una vasta gamma di algoritmi di analisi di rete, mentre Webgraph si distingue per la sua capacità di rappresentare grafi di grandi dimensioni

in modo compresso ed efficiente. Insieme, queste due librerie hanno permesso di eseguire analisi dettagliate sul grafo globale delle transazioni e sui chunk temporali, mantenendo un alto livello di efficienza anche su dataset di dimensioni massicce.

Le sezioni seguenti illustrano nel dettaglio il ruolo di Igraph e Webgraph nel progetto, descrivendo le loro funzionalità principali, le motivazioni per la loro scelta e il loro contributo all'analisi delle reti di stablecoin.

4.4.1 Igraph

Igraph è una libreria altamente specializzata per la creazione, manipolazione e analisi di grafi e reti complesse. Originariamente sviluppata per linguaggi come R, Python e C, la versione in C++ si distingue per la sua efficienza nell'analisi di grandi dataset, garantendo performance elevate e un ampio supporto per la computazione di metriche avanzate di rete [49]. Igraph è molto utilizzata in molteplici campi di ricerca come bioinformatica, analisi delle reti sociali, grafi transazionali eccetera.

Motivazioni per l'uso di Igraph

La scelta di Igraph per l'analisi delle reti ERC-20 è stata guidata da diversi fattori fondamentali come gestire dataset su larga scala come le reti di transazioni ERC-20 che sono caratterizzate da un numero elevato di nodi e archi, corrispondenti a milioni di indirizzi e transazioni. Igraph offre un'infrastruttura scalabile per gestire tali quantità di dati senza compromettere le performance [50]. È possibile calcolare con facilità metriche fondamentali per la comprensione della topologia della rete, come la centralità, la connessione tra nodi e il clustering.

I grafi delle transazioni ERC-20 sono stati costruiti utilizzando dati grezzi estratti della blockchain, in cui nodi rappresentano gli indirizzi e gli archi rappresentano le transazioni dirette tra di essi (Sezione 4.1). Igraph è stato utilizzato per creare questi grafi a partire da file con estensione *txt* attraverso le relative funzioni [51]. È stato utilizzato per calcolare misure come il Pagerank, identificazione delle componenti connesse e distribuzione dei gradi [52]. In particolare:

- Per i grafi globali ha permesso di ottenere una visione completa della rete di transazioni per ciascuna stablecoin, analizzando la struttura complessiva e identificando i nodi più centrali.
- Per i chunk temporali ha facilitato l'analisi delle variazioni nel tempo delle metriche di centralità e delle componenti connesse, permettendo di monitorare l'evoluzione delle reti di stablecoin in base a fattori esterni come la volatilità di mercato.

Grazie alla sua efficienza e flessibilità, Igraph ha consentito di condurre analisi su larga scala mantenendo un elevato livello di dettaglio e precisione. Questo strumento

è stato essenziale per la costruzione dei grafi e l'esecuzione di calcoli complessi, risultando fondamentale nell'interpretazione delle dinamiche transazionali tra i wallet delle stablecoin analizzate.

4.4.2 WebGraph

WebGraph è una libreria Java sviluppata principalmente per rappresentare e comprimere in modo efficiente grafi di grandi dimensioni [3]. Progettata originariamente per la rappresentazione di grafi del Web, la libreria è stata ideata per sfruttare le ridondanze strutturali presenti nei grafi, consentendo di immagazzinare e gestire reti estremamente ampie in memoria con un consumo minimo di risorse. Il framework offre strumenti avanzati per l'analisi e la manipolazione efficiente di grafi in formato compresso, permettendo di lavorare con dataset che altrimenti richiederebbero risorse computazionali elevate.

Le tecniche di compressione utilizzate da WebGraph, come la *referenziazione* e la *intervallazione*, permettono di rappresentare grafi con un'elevata efficienza sia in termini di spazio che di velocità di accesso ai dati [3]. Questa capacità rende WebGraph particolarmente adatta per l'analisi di reti di transazioni blockchain, dove i grafi risultano essere grandi e dinamici.

Motivazione per l'uso di WebGraph

L'uso di WebGraph nel contesto delle transazioni ERC-20 è stato guidato da diverse considerazioni come la gestione efficiente di grafi di grandi dimensioni, la capacità di rappresentare grafi sparsi e la disponibilità di strumenti per il calcolo di metriche avanzate.

La capacità di comprimere i grafi delle transazioni ERC-20 si è rivelata fondamentale per poter analizzare reti su larga scala. WebGraph, come detto, utilizza tecniche di compressione basate su *intervallazione* e *referenziazione* che riducono significativamente lo spazio richiesto per immagazzinare i dati, permettendo di mantenere la rete completa in memoria.

WebGraph permette di percorrere il grafo in modo rapido grazie a tecniche di iterazione *lazy*, che caricano solo i dati strettamente necessari al momento dell'accesso. Questa caratteristica ha reso possibile eseguire analisi su grafi compressi senza la necessità di decomprimerli completamente, migliorando notevolmente le prestazioni durante l'analisi di grandi volumi.

HyperBall

Webgraph ha strumenti avanzati come *HyperBall* [53], un algoritmo integrato nella libreria usato per misurare la distanza media tra i nodi e altre proprietà metriche di

reti molto grandi, come la *harmonic centrality* (Sezione 5.10), utilizzando una tecnica nota come **HyperLogLog** per stimare la distanza tra i nodi [54]. HyperBall sfrutta una combinazione tra la *propagazione iterativa* delle informazioni nel grafo e la *stima probabilistica* delle distanze, utilizzando *HyperLogLog* che calcola il numero di nodi raggiungibili da ogni nodo nella rete, basandosi su funzioni hash. Questo approccio consente di memorizzare e gestire solo un piccolo insieme di hash invece di dover conservare un elenco completo di tutti i nodi esplorati. Invece di espandere esplicitamente la ricerca a tutti i nodi connessi, HyperBall stima la distanza media tra i nodi in modo probabilistico, riducendo significativamente il consumo di memoria. HyperBall esegue una propagazione delle informazioni dal nodo di partenza ai suoi vicini, aggiornando i valori iterativamente fino alla convergenza. Una delle principali ragioni per cui HyperBall è stato scelto per il progetto è la sua scalabilità estrema. In [53] si dimostra che HyperBall è in grado di gestire centinaia di miliardi di nodi su sistemi con 2 TiB di RAM, cosa che lo rende ideale per l'analisi di reti enormi come quelle delle transazioni blockchain. Le tecniche di compressione di Webgraph, combinate con HyperBall, consentono di memorizzare e navigare enormi grafi in-core (in memoria) senza dover accedere frequentemente al disco, migliorando notevolmente la velocità di calcolo.

4.5 Conclusioni

L'integrazione di Igraph e Webgraph ha garantito un approccio ottimale e completo all'analisi delle reti di transazioni ERC-20. La combinazione di queste due librerie ha consentito di affrontare le sfide di scalabilità, gestione della complessità e analisi temporale, fornendo una visione chiara e dinamica dei flussi di valore all'interno delle reti stablecoin. Questa sinergia ha permesso di analizzare i grafi su più livelli, offrendo insight fondamentali sia a livello globale che su base temporale.

Capitolo 5

Framework per l'analisi

Questo capitolo illustra in modo approfondito le metriche calcolate per l'analisi delle reti transazionali ERC-20 del nostro caso di studio, evidenziando l'approccio metodologico adottato e i principi computazionali sottostanti. Le metriche descritte sono state selezionate per la loro rilevanza nel caratterizzare reti complesse, fornendo informazioni critiche sulla posizione e il ruolo dei nodi, sui flussi economici e sui pattern comportamentali. Tra queste troviamo misure classiche come il PageRank, gli score di Hub e Authority. Inoltre, si analizzano le distribuzioni di gradi, che permettano di studiare la struttura globale della rete e la concentrazione delle connessioni.

L'implementazione di queste metriche è stata sviluppata con un approccio rigoroso, sfruttando algoritmi consolidati e tecniche ottimizzate per gestire reti di grandi dimensioni con pesi multipli sugli archi. Particolare attenzione è stata posta nella combinazione e nella normalizzazione dei dati, garantendo una rappresentazione bilanciata tra frequenza e valore delle transazioni.

Questo capitolo fornisce una descrizione dettagliata del processo computazionale per ogni metrica, evidenziandone il significato teorico e pratico. L'obiettivo principale è mostrare come tali misure permettono di estrarre conoscenze approfondite sulle reti analizzate, dalle gerarchie strutturali alle dinamiche transazionali, offrendo un quadro completo delle interazioni tra gli agenti economici. Perciò, oltre a rappresentare contributo significativo alla comprensione delle reti ERC-20, questo capitolo stabilisce una solida base metodologica per studi futuri, fornendo strumenti avanzati per analizzare l'evoluzione delle rete transazionali in contesti decentralizzati e digitali.

5.1 Grado e Strength dei nodi

Il *grado* di un nodo in un grafo misura il numero di connessioni che esso ha con altri nodi. Nel nostro caso di un grafo diretto, possiamo distinguere tra *grado in entrata (in-degree)* il numero di archi che puntano verso il nodo ovvero il numero di transazioni ricevute, e il *grado in uscita (out-degree)* il numero di archi che partono dal nodo, rappresentando quindi il numero di transazioni inviate.

Il calcolo del grado è un'operazione essenziale per valutare la connettività e la posizione di un nodo all'interno della rete. Nelle reti di transazioni ERC-20, il grado può fornire indicazioni su indirizzi particolarmente attivi, sia come destinatari di numerose transazioni sia come mittenti.

La *forza (Strength)*, o meglio grado *pesato*, è un'estensione del concetto di grado che considera i pesi degli archi incidenti sul nodo. In questo contesto la *forza in entrata* somma tutti i valori di tutte le transazioni ricevute da un nodo. Questo indica quindi il totale dei token ricevuti in una determinata finestra temporale o nell'intero grafo globale di quel nodo. Mentre la *forza in uscita* somma i valori di tutte le transazioni inviate da un nodo, rappresentando quindi il totale dei token trasferiti a partire dal nodo. La forza permette di comprendere non solo la frequenza delle transazioni ma anche la loro rilevanza in termini di valore, risultando fondamentale in analisi di reti transazionali.

Calcolo dei gradi e della forza dei nodi nel nostro contesto

Per il multigrafo globale è stato calcolato il grado e la forza di ogni nodo attraverso funzioni predisposte da Igraph (Sezione 4.4.1) come descritto in precedenza.

Consideriamo il multigrafo rappresentato in Figura 4.1; ogni arco ha due pesi: il valore trasferito nella transazione e il timestamp. Ovviamente la forza sarà calcolata sul primo peso. Calcoliamo quindi i quattro parametri che sono: *Grado entrante*, *Grado uscente*, *Forza entrante* e *Forza uscente* per un nodo di esempio, il nodo A. Il nodo A riceve 2 transazioni da C con valori trasferiti di 90 e 190 ed una da B con valore 35, quindi il suo grado entrante sarà uguale a 3, mentre la sua forza entrante sarà pari a: $190 + 90 + 35 = 315$. Invia invece 2 transazioni a B con valori di 30 e 120 quindi avrà grado uscente pari a 2 e forza uscente pari a $120 + 30 = 150$. Nella Tabella 5.1 riassumiamo i risultati calcolati per ogni nodo del grafo di esempio.

Nei grafi di ciascun chunk temporale, poiché utilizziamo un grafo collassato in cui i pesi degli archi rappresentano la molteplicità delle transazioni tra due nodi e la somma dei valori trasferiti, abbiamo adottato una strategia specifica per calcolare grado e forza. In questo contesto, disponiamo già delle informazioni parziali di ogni nodo, come il grado parziale di un nodo con un altro nodo e la forza (ovvero, la somma dei valori delle transazioni).

Nodo	Grado Entrante	Grado Uscente	Forza Entrante	Forza Uscente
A	3	2	315	150
B	2	3	150	148
C	2	2	113	280

Tabella 5.1: Tabella riepilogativa dei gradi e delle forze dei nodi dell'esempio del multigrafo globale in Figura 4.1.

Per ottenere il grado totale e la forza totale entrante di un nodo, è sufficiente sommare rispettivamente tutti i pesi di molteplicità e le somme dei valori delle transazioni per gli archi in cui il nodo agisce come destinatario. Analogamente, la forza totale e il grado totale uscente si ottengono calcolando la somma di tutti i pesi relativi agli archi in cui il nodo funge da mittente.

Per chiarire meglio questo processo, consideriamo l'esempio illustrato in Figura 4.2, che rappresenta un grafo collassato di un chunk temporale. Come si può notare il nodo A effettua più trasferimenti verso B, E ed F. A questo punto il processo avviene in questa maniera: prendiamo tutte le transazioni in cui A è mittente:

- $A \rightarrow B$: ha peso $(10, 90000)$, ciò significa che A invia 90.000 token in 10 transazioni diverse a B.
- $A \rightarrow E$: ha peso $(2, 50)$, ciò significa che A invia 50 token in 2 transazioni diverse ad E.
- $A \rightarrow F$: ha peso $(3, 45)$, ciò significa che A invia 45 token in 3 transazioni diverse a C.

Perciò effettuando il processo descritto in precedenza, il nodo A avrà grado uscente pari a: $10 + 2 + 3 = 15$ e forza uscente pari a $90000 + 50 + 45 = 90095$.

Al contrario consideriamo le transazioni dove A è destinatario, quindi avremo:

- $F \rightarrow A$: ha peso $(1, 23)$, quindi c'è solo una transazione da F verso A con valore 23.

A questo punto è facile concludere che A ha grado entrante pari a 1 e forza entrante pari a 23. Ovviamente questo è stato solo un caso di esempio: viene fatto lo stesso procedimento per tutti i nodi. La Tabella 5.2 mostra i gradi e le forze per ogni nodo del grafo collassato di ogni chunk.

Nodo	Grado Entrante	Grado Uscente	Forza Entrante	Forza Uscente
A	1	3	23	90095
B	10	2	90000	14
C	9	10	12414	2792
D	6	20	1902	1000912
E	26	10	1001852	12445
F	7	1	135	23

Tabella 5.2: Tabella riepilogativa dei gradi e delle forze dei nodi dell'esempio del grafo collassato per i singoli chunk illustrato in Figura 4.2.

5.2 Analisi della distribuzione a power law

La **distribuzione power law** è una funzione che descrive fenomeni in cui la probabilità di osservare eventi rari e di grande entità decresce con andamento specifico, seguendo una relazione del tipo:

$$p(x) \propto x^{-\alpha}$$

dove α è un parametro noto come *esponente della power law*. Questa distribuzione, tipica di reti complesse come quelle di trasferimenti su blockchain, è caratterizzata da un comportamento **heavy-tailed**: solo pochi nodi accumulano la maggioranza delle connessioni o delle transazioni (funzionando da hub), mentre la maggior parte ha poche connessioni.

Per analizzare la distribuzione dei gradi dei nodi, abbiamo utilizzato **plfit**, un metodo statistico basato sul lavoro di *Clauset*, *Shalizi* e *Newman* [55]. Questo approccio combina metodi di *massima verosomiglianza* con testi di *goodness-of-fit* come il **Kolmogorov-Smirnov (KS)** e confronti tramite *rapporti di verosomiglianza* con modelli alternativi, permettendo un'analisi rigorosa e robusta della presenza di una power law [56]. Il metodo plfit è particolarmente efficace poiché riduce gli errori che possono insorgere da fluttuazioni nei valori estremi della distribuzione (la "*coda*"), e permette di identificare con precisione l'intervallo di valori $x \geq x_{min}$ in cui la power law è valida.

Nel nostro studio abbiamo applicato il plfit per caratterizzare la distribuzione dei gradi in ingresso e in uscita dei grafi temporali e globali delle transazioni ERC-20 dei quattro token presi come caso di studio: DAI, USDT, USDC e WETH. Per ogni grafo, plfit ha prodotto le seguenti statistiche:

1. **Esponente della power law** α: quantifica l'intensità della power law; un valore maggiore di α indica una distribuzione più concentrata attorno ai valori piccoli.

2. **Parametro** x_{min}: identifica il punto a partire dal quale i dati iniziano a seguire una distribuzione power law.

3. **Log-verosomiglianza (L)**: misura quanto bene il modello della power law si adatta ai dati.

4. **Distanza KS (D)**: calcola la massima distanza tra la distribuzione cumulativa osservata e quella teorica power law.

5. **P-value**: utilizzato per verificare se l'adattamento alla power law è statisticamente accettabile; un valore superiore a 0.1 indica che i dati possono plausibilmente seguire una power law.

L'analisi della distribuzione dei gradi tramite plfit consente di comprendere meglio la struttura della rete di transazioni. La presenza di una distribuzione power law nei gradi indica che la rete è altamente eterogenea, con pochi nodi che svolgono il ruolo di hub principali. Fornisce un'analisi robusta dei gradi, in quanto permette di verificare statisticamente se i dati osservati seguono una power law, evitandone l'uso inappropriato. Monitorando i parametri come α nel tempo, è possibile rilevare cambiamenti nella struttura della rete di transazioni ERC-20: una diminuzione di α potrebbe indicare una centralizzazione crescente (con più nodi che diventano "hub" transazionali), mentre un aumento suggerirebbe una distribuzione più decentralizzata delle transazioni. Questo approccio fornisce un quadro dettagliato della dinamica strutturale e permette di individuare tendenze di centralizzazione o decentralizzazione nel tempo

5.3 Componenti connesse

Le componenti connesse in un grafo rappresentano sottogruppi di nodi interconnessi, dove ciascun nodo è raggiungibile da ogni altro nodo all'interno della stessa componente. In ambito delle reti di transazioni ERC-20, l'analisi delle componenti connesse offre un'importante visione sulla struttura e connettività della rete, permettendo di comprendere la coesione dei partecipanti e identificare cluster di nodi con comportamenti correlati. Nelle reti orientate, come quelle del nostro caso di studio, esistono due principali tipologie di componenti connesse:

- **Strongly Connected Component (SCC)**: La componente fortemente connessa di un grafo è un sottoinisieme di nodi tale che, per ogni coppia di nodi u e v all'interno di questa componente, esiste sia un percorso diretto da u a v sia uno da v ad u. In altre parole, ogni nodo può raggiungere tutti gli altri nodi della stessa componente e viceversa.

- **Weakly Connected Component (WCC)**: La componente debolmente connessa include tutti i nodi che sono collegati tra loro se si considera il grafo come non orientato, ignorando la direzione degli archi.

Nel nostro contesto, le SCC e WCC forniscono intuizioni fondamentali sulla struttura e sul comportamento della rete. Analizzare SCC infatti può rilevare gruppi di indirizzi particolarmente interconnessi, suggerendo la presenza di comunità chiuse o cluster di nodi che partecipano a transazioni reciproche e frequenti. In alcuni casi, queste componenti potrebbero rappresentare insiemi di utenti che operano in gruppi coordinati o smart contract che interagiscono in maniera intensiva. Al contrario le WCC permettono di identificare insiemi più ampi di nodi che, anche se non reciprocamente connessi, fanno parte di una stessa "*comunità*" di scambio. Le WCC quindi permettono di osservare la rete da un punto di vista globale, identificando i nodi che contribuiscono al tessuto generale delle transazioni, anche se non mantengono una connettività reciproca.

Nella nostra analisi, ogni chunk temporale della rete viene trattato come un grafo separato, su cui si estraggono le SCC e le WCC più grandi. Per ogni chunk, grazie a l'uso di alcune funzioni fornite dalla libreria *Igraph* (Sezione 4.4.1), estraiamo la componente SCC e WCC più grande per ciascun grafo e calcoliamo la dimensione, ovvero il numero di nodi e archi, per entrambe le componenti. Una componente con molti archi rispetto ai nodi può indicare un'elevata connettività interna, e quindi un'alta densità (Sezione 5.4).

5.4 Densità

La densità di un grafo è una misura che indica quanto esso è vicino a essere completo, ossia quantifica le connessioni esistenti rispetto al numero massimo possibile di connessioni tra i nodi. Formalmente la densità di un grafo non orientato è definita come:

$$Density = \frac{2 \cdot |E|}{|V| \cdot \Big(|V| - 1\Big)}$$

Dove $|E|$ è il numero di archi e $|V|$ è il numero di nodi.

Nel nostro contesto un'alta densità può indicare un elevato grado di connettività, dove molti indirizzi interagiscono frequentemente tra loro. Questo suggerisce una rete ben integrata in cui i partecipanti tendono a scambiare token più liberamente. Al contrario, una bassa densità suggerisce che le interazioni sono meno frequenti, e quindi la rete è composta da sotto-gruppi con meno interazioni reciproche.

Nel nostro studio calcoliamo la densità per ogni chunk temporale. Questo permette di osservare l'evoluzione delle connettività nel tempo, identificando i periodi con maggiore o minore attività transazionale. Per il calcolo della densità dei chunk

temporali, utilizzare il grafo non orientato è una scelta strategica e sufficiente per i nostri obiettivi. Nel contesto delle transazioni ERC-20, infatti, l'interesse principale è valutare il livello complessivo di interconnessione tra i nodi in ogni periodo temporale, senza la necessità di considerare la direzione specifica delle transazioni.

5.5 Diametro

Il diametro di un grafo è una misura fondamentale in teoria dei grafi che rappresenta la massima distanza minima tra due nodi qualsiasi del grafo. In pratica, identifica la "lunghezza" del cammino minimo più lungo possibile tra coppie di noi, considerando solo i cammini più brevi disponibili.

In un contesto di grafo orientato come il nostro tiene conto della direzione degli archi e quindi una distanza è calcolabile solo se esiste un cammino diretto che collega un nodo ad un altro. Calcoliamo il diametro per ogni chunk temporale della rete ERC-20 usando il grafo diretto. Questo è utile per comprendere il livello di separazione all'interno di ogni chunk temporale, infatti rappresenta il massimo dei cammini minimi, espressa in numero di transazioni dirette, tra nodi in grado di comunicare tra loro. Questo approccio permette di analizzare dinamiche come l'estensione massima delle interazioni direzionali in ogni intervallo temporale.

Il diametro viene calcolato utilizzando una classe di `Webgraph` (Sezione 4.4.2) chiamata `SumSweepDirectedDiameterRadius`. Il metodo scelto, noto come "*sweeping*", è un'implementazione approssimata ma estremamente efficiente per il calcolo del diametro, indicata per grafi di grandi dimensioni [57]. Si applica il metodo di *sweeping* per ogni grafo diretto, che esegue una serie di visite all'interno del grafo e approssima il diametro con un numero di iterazioni ottimizzato per ridurre la complessità computazionale.

Un diametro ridotto può indicare una rete altamente connessa, mentre un diametro elevato potrebbe suggerire la presenza di sub-reti meno integrate. Mentre una rete con un diametro contenuto è generalmente più efficiente nelle comunicazioni, facilitando la diffusione dei token in pochi passaggi. Confrontare il diametro tra chunk successivi aiuta a rilevare cambiamenti nelle modalità di interazione tra indirizzi, come fasi di intensa attività o periodi di transazioni più frammentate.

5.6 Coefficiente di Clustering

Il coefficiente di clustering è una misura che quantifica quanto i nodi in una rete tendano a formare gruppi o "triangoli". Questo valore indica la probabilità che due vicini di un nodo siano anche vicini tra loro, creando una struttura di legami reciproci

o gruppi stretti. In altri termini, è un'indicazione di quanto sia "raggruppata" una rete attorno ai suoi nodi.

Duncan J. Watts e Steven Strogatz introdussero questa misura nel 1998 per determinare se un grafo sia o meno una rete rientrante nella teoria dello small world [58]. Per un nodo v, il coefficiente di clustering locale, indicato come C_v, misura quanto i suoi vicini siano anche connessi tra loro. È calcolato come:

$$C_v = \frac{2 \cdot e(v)}{k_v \cdot (k_v - 1)}$$

dove $e(v)$ è il numero di collegamenti effettivi tra i vicini del nodo v, e k_v il numero di vicini del nodo v. Questo valore è espresso tra 0 ed 1: se $C_v = 1$, tutti i vicini del nodo v sono collegati tra di loro, formando una "clique"; se $C_v = 0$, non c'è nessun collegamento tra i vicini di v.

Watts e *Strogatz* affermarono che le reti *small-world* sono caratterizzate da un alto coefficiente di clustering e una bassa distanza media tra i nodi. Nei grafi completamente casuali, il coefficiente di clustering tende a essere basso, mentre nei grafi regolari può essere molto alto. Le reti small-world sono un interessante via di mezzo, dove il clustering è mantenuto alto anche se la struttura è meno rigida e la distanza media tra i nodi rimane contenuta. Questa proprietà è presente in molte reti reali, come le reti sociali, le reti biologiche e reti di transazioni [58].

Coefficiente di clustering per le reti di transazioni ERC-20

Il clustering nel nostro contesto può essere utile per individuare comportamenti di gruppo o "*cluster*" di indirizzi che tendono a interagire frequentemente tra loro. Questo potrebbe suggerire dinamiche di mercato o gruppi di indirizzi che si scambiano valore regolarmente. In particolare calcoliamo il coefficiente di clustering globale come la somma di tutti i coefficienti locali divisa per il numero totale di nodi del grafo, o meglio la media dei coefficienti. Calcolare il valore globale per ogni chunk temporale di ogni token ci permette di ottenere una misura complessiva della "clusterizzazione" per ciascun intervallo di tempo considerato. Questo processo consente di osservare come la tendenza alla formazioni di gruppi di indirizzi interconnessi possa variare nel tempo.

5.7 Reciprocità

La **reciprocità** in un grafo diretto misura la probabilità che un arco diretto tra due nodi sia reciprocato da un altro arco in direzione opposta. Formalmente quantifica quanto il grafo si avvicini ad essere una struttura non orientata, dove per

ogni transazione unidirezionale esiste anche una controparte in senso opposto. Questo parametro è molto importante nell'analisi delle reti economiche decentralizzate, poiché può rivelare informazioni sulla simmetria delle interazioni finanziarie e sul comportamento transazionale dei partecipanti alla rete. In particolare nel nostro contesto, un alto valore di reciprocità indica una dinamica in cui gli utenti scambiano spesso valore bidirezionalmente, come potrebbe verificarsi tra indirizzi con rapporti commerciali stabili o tra individui che ricorrono a trasferimenti frequenti. Al contrario, un valore di reciprocità basso suggerisce interazioni più orientate in una singola direzione, tipiche di indirizzi che agiscono prevalentemente come intermediari o accumulatori di fondi.

La reciprocità è stata calcolata utilizzando la libreria `igraph`, specificamente tramite la funzione `igraph_reciprocity` che consente di calcolare il grado di reciprocità di un grafo diretto tramite la somma degli archi unidirezionali di come differisce dalla somma totale degli archi, normalizzando il valore in modo che 1 rappresenti un grafo completamente reciproco e 0 altrimenti.

5.8 Assortatività

Il coefficiente di assortatività, o assortatività di una rete, è una misura che indica quanto i nodi di una rete tendono a connettersi a nodi con proprietà simili, come il grado. Formalmente, il coefficiente di assortatività è definito come la correlazione di *Pearson* tra i gradi dei nodi connessi da un arco. Questa misura permette di identificare le strutture e le tendenze di connessione all'interno di una rete, rivelando se i nodi altamente connessi preferiscono formare legami con altri nodi di alto grado (rete assortativa) o con nodi di basso grado (rete disassortativa).

Matematicamente, il coefficiente di assortatività r si calcola come segue:

$$r = \frac{\sum_i (k_i - \bar{k})(k_j - \bar{k})}{\sum_i (k_i - \bar{k})^2}$$

dove k_i e k_j sono i gradi dei nodi connessi da ciascun arco e $\bar{k}$ è il grado medio dei nodi. Il coefficiente varia tra -1 e 1 e viene interpretato in questo modo:

- Valori positivi indicano assortatività, ovvero nodi di alto grado collegati ad altri nodi di alto grado.
- Valori negativi indicano disassortatività, ovvero nodi di alto grado collegati a nodi di basso grado.
- Valori vicini a zero suggeriscono una rete priva di tendenze specifiche nella connessione.

Un'analisi di questo tipo può aiutare a identificare reti assortative o disassortative, e questo è spesso indicativo della struttura di una rete economica decentralizzata, come evidenziato in [59].

Assortatività per le reti di transazioni ERC-20

Nel nostro caso di studio, il calcolo dell'assortatività nelle reti di transazioni ERC-20 viene effettuato sia rispetto ai gradi dei nodi sia rispetto alla loro forza (strength) (Sezione 5.1). Per comprendere meglio il significato e l'importanza di questa misura, analizziamo prima l'assortatività in base ai gradi, per poi analizzare la motivazione e il calcolo anche sulla forza.

In reti transazionali ERC-20, un valore elevato di assortatività in ingresso (*in-degree assortatvity*) significherebbe che indirizzi che ricevono molte transazioni tendono a connettersi con indirizzi simili, mentre un valore negativo indica che i indirizzi centrali tendono a collegarsi con indirizzi periferici.

Calcolare l'assortatività sulla strength del grafo permette di comprendere se i nodi trasferiscono o ricevono grandi volumi di token tendono a interagire con nodi simili. Questo calcolo è significativo poiché un'elevata assortatività in base alla forza potrebbe indicare tendenza dei indirizzi ad alto volume di transazioni a connettersi con altri indirizzi ad alto volume, suggerendo l'esistenza di hub centrali nel flusso di transazioni.

L'assortatività è stata calcolata sia per il grafo globale sia per in chunk temporali. In particolare abbiamo calcolato i gradi e la forza per i due tipi di grafi e li abbiamo utilizzati per il calcolo dell'assortatività in ingresso e in uscita sia per grado che per forza.

5.9 PageRank

Il PageRank è una delle misure più importanti e riconosciute per analizzare la centralità di un grafo, particolarmente nei contesti in cui le connessioni tra nodi riflettono l'importanza o il peso di ciascun nodo in base alle sue connessioni.

Questo concetto è nato in ambito web per classificare l'importanza delle pagine su Internet, come descritto per la prima volta nel famoso lavoro di *Sergey Brin* e *Lawrence Page* nel 1998 [60]. Il PageRank nasce come soluzione a uno dei problemi fondamentali del web: ordinare miliardi di pagine secondo la loro rilevanza. *Brin* e *Page* intuirono che il numero di collegamenti ipertestuali (link) tra le pagine poteva essere interpretato in modo simile alle citazioni accademiche. Le pagine con più link in ingresso (*backlinks*) erano ritenute più importanti, specialmente se tali link provenivano da altre pagine autorevoli. Da questa intuizione emerse l'idea di considerare ogni link come una sorta di "voto" di importanza e di determinare la centralità di

una pagina non solo dal numero di link ricevuti, ma anche dalla qualità di questi link, dove i voti di pagine già autorevoli pesano di più.

Dal punto di vista matematico, il valore del PageRank è definito come una misura iterativa basata su una distribuzione stazionaria di un "*random surfer*" all'interno di un grafo diretto. L'idea è che un utente ipotetico (surfer) scelga casualmente i collegamenti da seguire e, periodicamente, si "annoia" e si sposta su una nuova pagina scelta casualmente. Questo concetto è espresso tramite un'equazione che bilancia il peso tra i link entranti e il salto casuale, garantendo così che nessun nodo diventi una trappola senza uscita, una condizione nota come *rank sink*.

Uso nel nostro contesto

Il PageRank è essenziale nel nostro contesto di analisi delle transazioni ERC-20, in particolare per comprendere l'importanza relativa dei vari nodi (indirizzi) all'interno della rete delle stablecoin. Ci consente di misurare non solo la frequenza delle transazioni, ma anche il ruolo di un nodo come intermediario o punto di arrivo di flussi economici rilevanti. Viene evidenziato il suo utilizzo nel contesto blockchain per distinguere nodi di alto valore e per analizzare le reti decentralizzate di token, come dimostrato anche in studi recenti [61]. Questi nodi potrebbero essere grandi exchange o smart contract rilevanti. Monitorare l'evoluzione della centralità di questi nodi nel tempo è un'ottima soluzione per analizzare la stabilità di un nodo nel tempo.

Calcolo del PageRank per i due grafi

Qui il calcolo del PageRank è eseguito utilizzando l'algoritmo *PRPACK*, un algoritmo efficiente per la risoluzione di problemi di PageRank ottimizzato per grafi grandi e sparsi, come quelli del nostro caso di studio. Riduce il tempo di calcolo sfruttando tecniche di decomposizione iterativa per approssimare il vettore di PageRank [62]. Il *dumping factor* viene impostato a 0.85, un valore standard utilizzato nell'algoritmo di PageRank che tiene conto della probabilità che un nodo segua un collegamento oppure scelga un altro nodo a caso.

Il calcolo del PageRank, nella sua forma standard, non è in grado di gestire correttamente i multiarchi: l'algoritmo infatti considera la presenza o assenza di una connessione tra i nodi, ma non il numero o il peso specifico di questi collegamenti. Per questo abbiamo deciso di collassare il multigrafo globale per eseguire il calcolo del PageRank per ogni nodo, che tenga conto della reale intensità e frequenza delle interazioni tra i nodi come discusso nella Sezione 4.2.1. Dopo il collasso del multigrafo, il PageRank viene calcolato utilizzando il grafo pesato risultante. Questo significa che ogni arco tra due nodi contiene le informazioni aggregate alle loro transazioni. Abbiamo utilizzato la molteplicità delle transazioni come peso principale per influenzare il calcolo del PageRank. Tuttavia, anche la distribuzione temporale

delle transazioni gioca un ruolo importante: nodi che ricevono transazioni frequenti in un intervallo di tempo limitato sono trattati diversamente rispetto a nodi con un volume simile di transazioni distribuito su periodi più lunghi. In altre parole, la frequenza consente di individuare nodi che mostrano un'attività più concentrata e intensa. L'algoritmo `PRPACK` utilizza i pesi per determinare quanto "importante" è un collegamento tra due nodi. In pratica, un nodo che riceve molte transazioni pesanti da nodi influenti dipende non solo dal numero di connessioni, ma anche dalla loro qualità, espressa in termini di frequenza delle transazioni. Ciò ci da una maggiore precisione perché i nodi che hanno molteplici interazioni con altri nodi non sono considerati equivalenti a quelli con poche transazioni, ma vengono trattati in base alla quantità reale delle transazioni. Questo rappresenta meglio la centralità economica di un nodo nella rete.

Abbiamo personalizzato l'algoritmo di PageRank per utilizzare questi pesi attraverso una funzione che mette a disposizione *Igraph* (Sezione 4.4.1): `igraph_personalized_pagerank()` [52]. Senza questa personalizzazione, il PageRank verrebbe calcolato in modo uniforme, ossia ogni collegamento avrebbe lo stesso peso, indipendentemente da quante transazioni siano state trasferite tra due nodi. Abbiamo potuto rappresentare l'intensità delle relazioni tra i nodi, assegnando un peso più alto a quei collegamenti che riflettono una maggiore molteplicità. L'effetto di questa personalizzazione è che i nodi con collegamenti più forti influenzeranno maggiormente il risultato del PageRank.

Per spiegare meglio il funzionamento del PageRank applicato al grafo globale, prendiamo come riferimento il caso illustrato nella Figura 4.1, che rappresenta un multigrafo globale, e una volta collassato otteniamo un grafo ponderato con tre nodi principali: A, B e C. Ora guardiamo attentamente come questo incide nel calcolo del PageRank:

- Il nodo A riceve una transazione da B e due transazioni da C, per un totale di 3 collegamenti entranti. Riceve il maggior numero di collegamenti in ingresso e di conseguenza otterrà un PageRank più elevato.

- Il nodo B ha un PageRank moderato, poiché riceve 2 transazioni da A, ma invia anche transazioni sia a C che ad A, distribuendo parte della sua importanza.

- Il nodo C riceve due transazioni da B, il che conferisce un PageRank discreto, ma inferiore a quello di A, poiché riceve da un solo nodo (B).

Nella Figura 5.1 un esempio di grafo globale collassato dove la dimensione dei nodi è proporzionale al loro PageRank. L'analisi visiva dei nodi ci offre una chiara rappresentazione della loro centralità della rete basata sulle interazioni e sui flussi di transazioni. Possiamo concludere che il nodo A emerge come il nodo con il

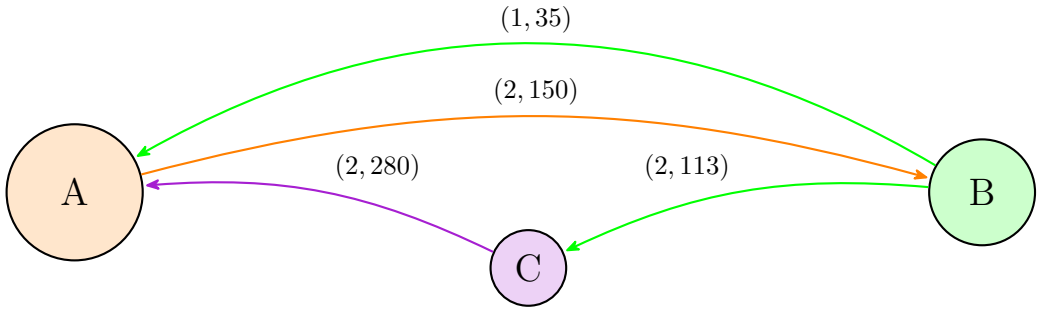


Figura 5.1: Esempio della struttura del grafo globale collassato ponderato con dimensione variabile dei nodi in base al PageRank.

PageRank più alto, grazie ai suoi tre collegamenti in entrata. Il nodo B ha una dimensione intermedia, riflettendo la sua importanza, pur avendo solo due collegamenti in entrata, ma ricevendo da A, che è un nodo centrale. Il nodo C, con due collegamenti entranti da B, ha una dimensione inferiore rispetto ad A, ma rimane comunque un nodo attivo e influente. L'analisi del PageRank in questo grafo globale dimostra che la centralità dei nodi dipende fortemente dal numero e dalla qualità delle transazioni in ingresso.

Analogamente quanto fatto per il grafo globale, i grafi temporali, che sono stati collassati in principio, hanno seguito la stessa logica di calcolo. Questo processo ha consentito di mantenere coerenza nel calcolo sia a livello globale che temporale, sfruttando l'intensità delle connessioni come misura di centralità economica di ciascun nodo.

5.10 Harmonic centrality

L'harmonic centrality misura la vicinanza di un nodo rispetto agli altri in un grafo, superando alcune limitazioni della *Closeness centrality*, specialmente nei grafi non connessi. Mentre la Closeness centrality calcola l'inverso della somma delle distanze di un nodo rispetto agli altri, l'harmonic centrality invece somma direttamente gli inversi delle distanze. Questo approccio evita di produrre valori infiniti in grafi con componenti non connesse e fornisce una misura più informativa sulla raggiungibilità relativa di ogni nodo rispetto agli altri, anche in strutture parzialmente connesse. Nel caso di una rete non connessa, un nodo isolato avrebbe una harmonic centrality pari a zero, ma nodi in piccoli cluster ben connessi otterrebbero comunque un punteggio positivo. Questo rende l'harmonic centrality particolarmente utile per grafi di tipo transazionale dove le connessioni potrebbero non essere uniformemente distribuite, ma sono comunque significative delle comunità o dei cluster.

Formalmente, come descritto in [63], l'harmonic centrality per un nodo x_i è definita come:

$$c_H(x_i) = \sum_{j \neq i} \frac{1}{dist(x_i, x_j)}$$

dove $dist(x_i, x_j)$ è la distanza *geodetica* (cioè il cammino più breve) tra i nodi x_i e x_j. Se un nodo j è irraggiungibile da x_i, l'inverso della distanza viene considerato 0. Questa somma produce un valore di harmonic centrality che è tanto più alto quanto più un nodo è vicino, in media, agli altri nodi nel grafo. L'harmonic centrality normalizza così le distanze dovute alla connessione o meno di nodi in componenti isolate.

Applicazione al contesto delle reti di transazioni ERC-20

Nelle reti di transazioni ERC-20, l'harmonic centrality è un indicatore prezioso per identificare nodi rilevanti all'interno di cluster locali. Questo tipo di centralità mette in risalto nodi che, pur non essendo facilmente accessibili a livello globale, sono molto vicini ai nodi del proprio cluster. Ciò può indicare che alcuni indirizzi o smart contract fungono da hub in specifici sottogruppi, facilitando scambi frequenti e flussi di capitale tra indirizzi correlati.

indirizzi con alta harmonic centrality risultano accessibili rapidamente dai nodi locali, suggerendo una funzione di "gateway"[1] per la liquidità e una frequente accessibilità locale, tipica di nodi operativi come piattaforme di scambio decentralizzate o indirizzi utilizzata per attività di alto volume di scambi.

Le reti di transazioni ERC-20 non sono completamente connesse, e i indirizzi tendono a raggrupparsi in componenti separate o cluster di attività. L'harmonic centrality si adatta bene a questo tipo di struttura perché, a differenza della Closeness centrality tradizionale, non risente negativamente dell'assenza di connessioni globali, offrendo così una misura della rilevanza locale anche in sottogruppi isolati.

Calcolo della centralità nel nostro studio

Per condurre questa analisi in modo efficiente, abbiamo implementato una strategia utilizzando Webgraph, in particolare la classe `HyperBall`, la quale permette un calcolo approssimato dell'harmonic centrality su grafi di grandi dimensioni, come spiegato nella Sezione 4.4.2.

L'approccio approssimato offerto da `HyperBall` è stato scelto per affrontare le sfide computazionali poste dalle reti ERC-20, che sono molto ampie e dense. Ogni grafo

[1] Un gateway si riferisce a un nodo che facilita il flusso di token tra diversi indirizzi o sottogruppi di una rete. Agisce come punto di accesso privilegiato per le transazioni, spesso accelerando il trasferimento di fondi e riducendo i tempi di attesa per i nodi connessi.

rappresenta transazioni su un intervallo temporale significativo, e il volume complessivo di dati accumulati, specialmente in grafi globali, richiede algoritmi scalabili per ottenere tempi di esecuzione praticabili. I metodi esatti per il calcolo dell'harmonic centrality, pur accurati, sono computazionalmente intensivi e non ideonei a reti con decine di milioni di nodi e archi. Di conseguenza `HyperBall` sfrutta tecniche basate su *HyperLogLog* per calcolare la somma delle distanze inverse approssimate, fornendo valori di harmonic centrality vicini che approssimano quella reale ad un costo computazionale ridotto.

Il processo impiega una serie di iterazioni per stimare la distanza di ciascun nodo rispetto agli altri, utilizzando un algoritmo di tipo *propagation* che calcola la somma delle distanze inverse senza dover memorizzare tutte le distanze esatte tra i nodi. In questo caso, `HyperBall` opera direttamente sul grafo direzionale caricato tramite `ImmutableGraph`. Il processo iterativo continua fino al raggiungimento di uno stato stazionario, determinato dall'assenza di modifiche significative tra iterazioni successive.

Eseguiamo il calcolo dell'harmonic centrality per entrambi i grafi di interesse, ovvero il grafo globale e i chunk temporali, entrambi collassati, al fine di ottenere una misura precisa della raggiungibilità dei nodi all'interno della rete ERC-20. Ciò consente di osservare variazioni dinamiche della raggiungibilità dei nodi nel tempo ed identificare i momenti in cui specifici nodi diventano più centrali o accessibili, permettendo di riconoscere pattern di comportamento ciclico o di picco nelle interazioni tra indirizzi e smart contract.

5.11 Hub e Authority Score

Hub e Authority Score sono misure di centralità che si utilizzano principalmente per comprendere la struttura e le relazioni di rete in grafi diretti. Inizialmente proposte nell'algoritmo *HITS* (*Hyperlink-Induced Topic Search*), queste metriche valutano la centralità dei nodi non in modo isolato, ma in base al ruolo che rivestono nelle relazioni con altri nodi della rete, analizzando come i nodi si influenzano reciprocamente in termini di connessioni direzionali.

HITS è stato originariamente sviluppato da *Jon M. Kleinberg* [64] per analizzare il *ranking delle pagine web*. I nodi authority sono nodi che ricevono molti link da hub, rappresentando così risorse autorevoli, mentre i nodi hub sono quelli che puntano a molte authority, fungendo da connettori o "raccomandatori". Questo modello crea una struttura gerarchica dove i nodi hub identificano e puntano alle risorse più importanti, le authority, che risultano quindi centrali e influenti all'interno della rete. L'algoritmo si basa sull'idea di aggiornare iterativamente i punteggi di hub e authority di ogni nodo, fino alla convergenza. Funziona attraverso i seguenti passaggi principali:

- **Matrice di adiacenza e iterazioni**: A partire da una matrice di adiacenza A di un grafo diretto, HITS calcola gli Hub e Authority e in modo iterativo. Ogni nodo ha un Hub score $h(i)$ e di Authority score $a(i)$, inizializzati a valori casuali o uniformi.

- **Calcolo di Authority**: Per ciascun nodo i, il suo Authority score $a(i)$ viene aggiornato sommando gli Hub score di tutti i nodi che puntano a i. Formalmente:
$$a(i) = \sum_{j:j\to i} h(j)$$
o, in forma matriciale, utilizzando A^T la matrice trasposta: $a = A^T h$

- **Calcolo di Hub**: Allo stesso modo, l'Hub score $h(i)$ di ogni nodo viene aggiornato sommando gli Authority score di tutti i nodi a cui punta i. Questo passaggio viene calcolato come:
$$h(i) = \sum_{j:i\to j} a(j)$$
rappresentato come $h = Aa$ in notazione matriciale.

- **Convergenza e Normalizzazione**: Dopo ogni iterazione, i vettori a e h vengono normalizzati per evitare che i valori crescano indefinitamente. Il processo viene ripetuto fino a raggiungere la convergenza, quando gli Hub e Authority score non cambiano più significativamente tra una iterazione e la successiva.

Il risultato finale sono due insiemi di valori, rispettivamente per gli hub e per le authority, che permettono di identificare i nodi centrali nella rete.

Lo studio di *Patrick Doreian* [65] fornisce una rappresentazione visiva dell'importanza degli score di Hub e Authority all'interno di una rete sociale complessa, utilizzando un'analisi basata su HITS. In questa analisi, vengono individuati e visualizzati i principali nodi hub e authority per mostrare come questi si posizionano al centro della rete e fungano da snodi principali di connessione con nodi periferici. Questa metodologia ha come obiettivo l'identificazione dei nodi che centralizzano le connessioni, aiutando a evidenziare le gerarchie all'interno della rete: un nodo con un alto Authority score potrebbe rappresentare un indirizzi o uno smart contract che riceve una grande quantità di flussi, rendendolo punto di aggregazione o di attenzione per le transazioni, mentre un nodo con un alto Hub score potrebbe fungere da intermediario che distribuisce valore verso vari nodi di authority, indicandone l'importanza come "font" all'interno della rete.

Calcolo degli score per i nostri grafi

Per il calcolo degli score di Hub e Authority utilizziamo il grafo globale collassato, come fatto per il calcolo del PageRank. Questo approccio si rende necessario poiché l'algoritmo di HITS non è in grado di gestire multiarchi, ma considera di un singolo arco tra ogni coppia di nodi. Utilizziamo una funzione di `Igraph` che in base ai due pesi del grafo, calcola gli Hub e Authority Score per in due passaggi distinti:

1. **Calcolo degli score con la molteplicità**: Utilizziamo il primo peso, la molteplicità, per eseguire una stima iniziale degli score di Hub e Authority. Un nodo che riceve molte transazioni (e quindi ha una molteplicità elevata per gli archi in ingresso) avrà un Authority score più alto. Allo stesso modo, un nodo che invia molte transazioni avrà un Hub score più alto.

2. **Calcolo degli score con la somma dei valori trasferiti**: Utilizziamo il secondo peso, la somma dei valori trasferiti tra due nodi, per tenere conto dell'ammontare complessivo delle transazioni in ingresso e in uscita influenzando maggiormente i nodi che ricevono o inviano grandi volumi di transazioni.

Una volta ottenuti due insiemi di score (uno per ciascun peso), vengono combinati usando la somma logaritmica, che consente di tenere conto sia della frequenza delle transazioni (molteplicità) sia del valore complessivo trasferito. Questo meccanismo è spiegato più dettagliatamente nella Sezione successiva.

5.11.1 Somma logaritmica per Hub e Authority score

Utilizziamo la somma logaritmica per combinare efficientemente i due diversi pesi per gli archi. Questo approccio è cruciale per ottenere una misura equilibrata degli score di Hub e Authority, che rifletta tanto la frequenza quanto il valore delle transazioni tra i nodi.

La somma logaritmica è una tecnica di aggregazione che consente di combinare due valori in modo attenuato, riducendo l'impatto di valori estremamente alti e mantenendo una scala gestibile per il confronto tra i nodi. In formula, la somma logaritmica di due valori x e y è:

$$Somma\ Logaritmica = log(1 + x) + log(1 + y)$$

L'uso del logaritmo riduce il peso relativo di valori molto grandi, evitando che un singolo nodo con un valore eccezionalmente elevato domini il risultato finale. Nel nostro caso applicheremo la somma logaritmica per combinare due serie di score di Hub e Autohrity calcolati separatamente ovvero:

- **Score basati su molteplicità**

- **Score basati sulla somma dei valori trasferiti**

Quindi per ogni nodo il valore finale combinato per gli score di Hub e Authority viene calcolato con:

$$Hub = log(1 + Hub\ Score\ Molteplicita') + log(1 + Hub\ Score\ Somma\ Valori)$$

$$Authority = log(1 + Authority\ Score\ Molteplicita') + log(1 + Authority\ Score\ Somma\ Valori)$$

In una rete di transazioni, alcuni nodi possono inviare e ricevere molte transazioni a basso valore, mentre altri possono avere poche transazioni di valore elevato. La somma logaritmica permette di rappresentare entrambi i comportamenti in modo proporzionato, senza favorire eccessivamente né i nodi con molte transazioni né quelli con poche transazioni di grande valore.

5.12 Conclusioni

In conclusione, questa implementazione, ha portato a una raccolta e analisi dettagliata di statistiche di rete che permettono una comprensione approfondita delle dinamiche sottostanti nelle reti di transazioni ERC-20, con un focus sui token DAI, USDT, USDC e WETH. Ogni metrica è stata scelta per la sua capacità di evidenziare caratteristiche specifiche della struttura della rete, della centralità dei nodi, e dei flussi economici, contribuendo a una visione complessiva dell'evoluzione di queste reti nel tempo. L'uso di chunk temporali per suddividere il dataset permette di osservare i cambiamenti strutturali in una finestra temporale continua, monitorando come nodi e connessioni si evolvono in risposta ad eventi di mercato, politiche monetarie o strategie economiche di specifici attori. In particolare, il calcolo delle metriche di centralità, come il Pagerank, l'Hub e Authority Score e l'harmonic centrality, ci consente di identificare nodi influenti che possono fungere da hub transazionali o che posseggono una funzione di intermediazione economica. L'analisi delle componenti connesse, con l'estrapolazione delle componenti SCC o WCC più grandi, fornisce un'idea chiara di come gli utenti e gli smart contract interagiscono e si aggregano in comunità di scambio, mentre il calcolo della distribuzione power law sui gradi offre una misura della concentrazione e della distribuzione dei gradi tra i nodi.

In definitiva, il lavoro svolto pone le basi per un'analisi avanzata delle transazioni ERC-20, fornendo strumenti per monitorare, caratterizzare e potenzialmente prevedere l'andamento delle reti di token, dove è possibile confrontare il nostro approccio con studi precedenti come [31] e [66], offrendo al contempo una nuova prospettiva sulle dinamiche economiche decentralizzate.

Capitolo 6

Risultati sperimentali

In questo capitolo mostriamo i risultati sperimentali ottenuti dal calcolo delle statistiche di rete sui grafi delle transazioni ERC-20. Utilizzando le metriche introdotte e calcolate nel capitolo precedente, forniamo una visione complessiva del comportamento della rete di transazioni nel tempo. Esaminiamo in dettaglio i grafici ottenuti per ciascuna metrica, evidenziando i trend temporali, le differenze tra i diversi token e i comportamenti peculiari dei nodi centrali. Discuteremo infine l'importanza di queste osservazioni nel contesto delle stablecoin e delle dinamiche di trasferimento dei token, individuando i potenziali punti di interesse per approfondimenti futuri.

6.1 Il dataset

L'analisi si basa su un dataset tratto dal lavoro di [31], in cui vengono studiate le reti relative ai 100 token ERC-20 con il più alto numero di trasferimenti. Questo dataset è stato adattato e utilizzato per lo studio delle transazioni tra indirizzi, rappresentate come un grafo diretto e pesato, con particolare attenzione a quattro token ERC-20: DAI, USDT, USDC e WETH. Il dataset considerato contiene informazioni sugli eventi *Transfer* emessi dai contratti ERC-20 sulla blockchain di Ethereum, coprendo un arco temporale che va dal blocco 0, creato il 30 luglio 2015, fino al blocco 14 999 999, aggiunto il 21 giugno 2022. Il dataset rappresenta uno dei più completi insiemi di dati disponibili per lo studio delle transazioni basate su token fungibili ERC-20, e la sua struttura si adatta perfettamente all'analisi tramite grafi.

6.1.1 Struttura del dataset

Il dataset è organizzato in vari file CSV compressi in formato XZ per ottimizzare lo spazio, e contiene informazioni cruciali per modellare e analizzare le reti di

transazioni. I file rilevanti per il nostro studio sulle transazioni ERC-20 sono i seguenti:

- `block_timestamps_0-14999999.csv.xz`: Questo file fornisce informazione sui timestamp dei blocchi. Ogni riga rappresenta un blocco e contiene l'identificatore del blocco (altezza del blocco) e il timestamp in formato Unix[1] (epoch), che indica l'istante in cui il blocco è stato aggiunto alla blockchain.

- `erc20_transfers.csv.xz`: Questo è il file principale per l'analisi delle transazioni ERC-20 e contiene informazioni su ogni evento di trasferimento di token ERC-20. Le colonne rilevanti sono l'identificatore del blocco in cui è avvenuta la transazione; identificatore numerico del contratto ERC-20 che ha emesso l'evento di trasferimento; identificatore numerico del mittente del trasferimento; identificatore numerico del destinatario.

- `erc20_contracts.csv.xz`: Questo file contiene le informazioni sui contratti ERC-20 che hanno emesso almeno un evento di trasferimento all'interno dell'intervallo dei blocchi considerati. Ogni riga contiene l'indirizzo Ethereum del contratto ERC-20 e l'identificatore numerico utilizzato per rappresentare il contratto nel file delle transazioni.

- `erc20_addresses.csv.xz`: Raccoglie gli indirizzi Ethereum dei partecipanti coinvolti in almeno una transazione ERC-20. Ogni riga è composta dall'indirizzo dell'account Ethereum e l'identificatore numerico associato a ciascun partecipante, che viene poi utilizzato nel file delle transazioni.

- `erc20_values_dec.csv.xz`: Questo file contiene l'importo di token ERC-20 trasferiti per ogni transazione. Ogni riga del file corrisponde a una transazione registrata nel file `erc20_transfers.csv.xz`, e contiene l'ammontare di token scambiato.

Il nostro approccio ha sfruttato diverse tecniche per la costruzione dei grafi, a partire dal filtraggio dei dati per specifici contratti, per poi passare alla costruzione di grafi globali (Sezione 4.2) e alla suddivisione delle transazioni in chunk temporali mensili (Sezione 4.3).

Per garantire un'analisi focalizzata sui quattro token scelti per l'analisi, abbiamo selezionato solo le transazioni emesse dagli smart contract associati a USDT, USDC, WETH e DAI, utilizzando gli indirizzi univoci di ciascuna di esse per filtrare i dati. Questo filtraggio ha permesso di semplificare il processo di modellazione, consentendo la costruzione di grafi diretti in cui i nodi rappresentano gli indirizzi

[1]Misura il tempo in base al numero di secondi non intercalari trascorsi dalle 00 : 00 : 00 UTC del 1 gennaio 1970, l' epoca Unix. Nell'informatica moderna, i valori sono talvolta memorizzati con una granularità maggiore , come microsecondi o nanosecondi.

coinvolti e gli archi rappresentano le transazioni tra mittente e destinatario, come spiegato nella Sezione 4.1.

Un'ottimizzazione fondamentale nel processo di modellazione è stata l'assegnazione di identificatori numerici univoci a ciascun indirizzo. Poiché gli indirizzi Ethereum sono stringhe alfanumeriche lunghe, il loro utilizzo diretto nei grafi avrebbe comportato un notevole overhead computazionale. Convertendo gli indirizzi in identificatori numerici, abbiamo ridotto la complessità computazionale, migliorando la gestione e la velocità di accesso ai dati. Questa scelta è stata particolarmente utile nella costruzione di grafi di grandi dimensioni, poiché ha facilitato il processo di aggiornamento e manipolazione dei dati durante le fasi di analisi e calcolo delle statistiche.

Dopo aver filtrato le transazioni e assegnato gli identificatori numerici ai wallet, abbiamo costruito i grafi globali per ciascun token. Per la suddivisione dei dati di trasferimento in chunk temporali mensili abbiamo utilizzato il file `block_timestamps_-0-14999999.csv.xz` e `erc20_transfers.csv.xz` per mappare ogni trasferimento con il suo relativo timestamp attraverso l'identificativo del blocco.

Token	N° chunk	Periodo di inizio
DAI	32	Novembre 2019
USDT	58	Febbraio 2016
USDC	46	Settembre 2018
WETH	56	Aprile 2016

Tabella 6.1: Numero di chunk prodotti dopo la suddivisione mensile in finestre temporali e periodo iniziale per ogni token

La Tabella 6.1 riassume il numero di chunk ottenuti per ciascun token con il nome del primo chunk individuato, ovvero il momento in cui è avvenuta la prima transazione per quel token. Si può notare che i token non condividono lo stesso numero di chunk e le stesse date di inizio, riflettendo la diversità delle reti e dell'utilizzo di tali token.

6.2 Analisi strutturale e topologica

6.2.1 Cardinalità dei nodi e degli archi

In questa sezione analizziamo la cardinalità dei nodi e degli archi, ovvero il loro numero totale. In particolare, ci concentriamo sulla dimensione delle reti globali, in termini di trasferimenti e partecipanti, confrontandole con le loro evoluzioni temporali.

La Tabella 6.2 fornisce una panoramica del numero di nodi e archi per ciascun token, presentando i dati sia per il multigrafo globale, che include le transazioni ripetute tra le stesse coppie di nodi, sia per il grafo globale collassato, dove ogni coppia di nodi è rappresentata da un unico arco. Sebbene WETH non sia tecnicamente una stablecoin, questa può essere considerata una "quasi stablecoin" collateralizzata con una criptovaluta (ovvero Ether). WETH è inclusa nella nostra analisi perché svolge un ruolo cruciale nelle applicazioni di finanza decentralizzata, dove è spesso utilizzato come collaterale e strumento di scambio. Inoltre è interessante come varia la struttura che caratterizza questa rete, implicando quindi un confronto con le stablecoin. In particolare, WETH ha una struttura di rete distintiva caratterizzata da un numero relativamente ridotto di nodi (1.1 milioni) ma con un volume di transazioni molto elevato.

Token	N° nodi	N° Archi	N° Archi (unici)
DAI	1 749 967	13 649 738	4 011 225
USDT	23 176 195	149 404 179	66 902 205
USDC	8 235 862	42 463 753	18 020 579
WETH	1 121 372	104 183 064	4 611 611

Tabella 6.2: Numero di nodi e archi per ciascun token nei grafi non collassati (multigrafo) e collassati

Dalla tabella, inoltre, USDT risulta il token con il maggior numero di nodi (circa 23 milioni) e archi (circa 149 milioni nel multigrafo), un dato che riflette un utilizzo ampio e distribuito nelle rete Ethereum. Il numero elevato di transazioni, anche nel grafo collassato (circa 67 milioni di archi unici), suggerisce che USDT è utilizzato in modo capillare e regolare, probabilmente da una base di utenti vasta e diversificata. USDC mostra una struttura simile, con 8.2 milioni di nodi e 42 milioni di archi totali, sebbene con dimensioni inferiori rispetto a USDT, indicando comunque una domanda stabile e un utilizzo diffuso. DAI, con 1.7 milioni di nodi e circa 13.6 milioni di archi nel multigrafo, risulta più concentrato rispetto a USDT e USDC. D'altra parte WETH si distingue nettamente dagli altri token, con solo 1.1 milioni di nodi, ma un numero di archi molto alto, pari a 104 milioni nel multigrafo e ridotto a circa 4.6 milioni nel grafo collassato. Pur avendo pochi nodi rispetto agli altri token, questi partecipano a un numero di transazioni estremamente elevato con frequenti interazioni ripetute tra loro. Questo suggerisce che WETH opera in un contesto di rete più denso e intensivo per la sua compatibilità con lo standard ERC-20, che permette una facile integrazione con contratti DeFi [67]. Inoltre con la nascita di protocolli "*lending/borrowing*" come *Aave*, potrebbe essere utilizzato

come collaterale per prendere in prestito (lending) stablecoin per poi restituirle in futuro (borrowing), riottenendo il collaterale in WETH [68].

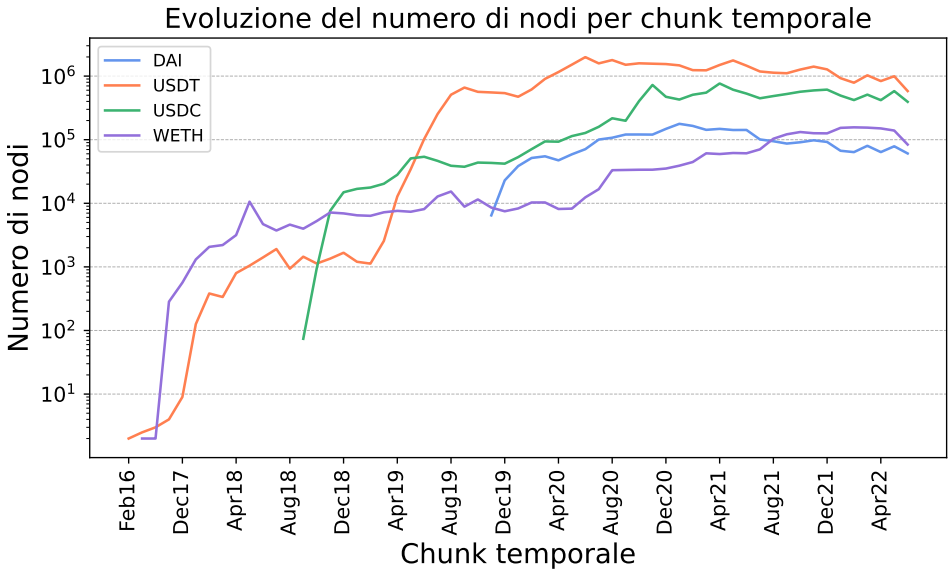


Figura 6.1: Evoluzione del numero di nodi per ogni token.

Le Figure 6.1 e 6.2 mostrano l'evoluzione temporale della cardinalità dei nodi e degli archi. Inizialmente, tutti i token mostrano una crescita rapida, con un forte aumento di entrambe le metriche. DAI presenta una crescita più graduale, probabilmente per la sua adozione progressiva nei protocolli DeFi e la necessità di sovra-collateralizzazione. Per WETH, la stabilizzazione anticipata del numero di nodi potrebbe essere dovuta dalla sua funzione specifica in pool di liquidità e smart contract, dove il numero di attori è più limitato ma altamente attivo. Con il passare del tempo vediamo che il numero di nodi e archi tende a stabilizzarsi per ciascun token, suggerendo che la rete ha raggiunto una fase di maturità, dove la crescita rallenta e si assesta su livelli più stabili, coerente con una stabilizzazione dell'adozione, in cui la base di utenti si consolida e l'attività transazionale mantiene un livello costante. Durante questo periodo si osservano comunque *picchi occasionali*, che indicano momenti di attività particolarmente intensa. Tali picchi sono probabilmente legati a eventi di mercato, o un utilizzo specifico dei token in contesti come la DeFi, o periodi di maggiore volatilità del mercato cripto.

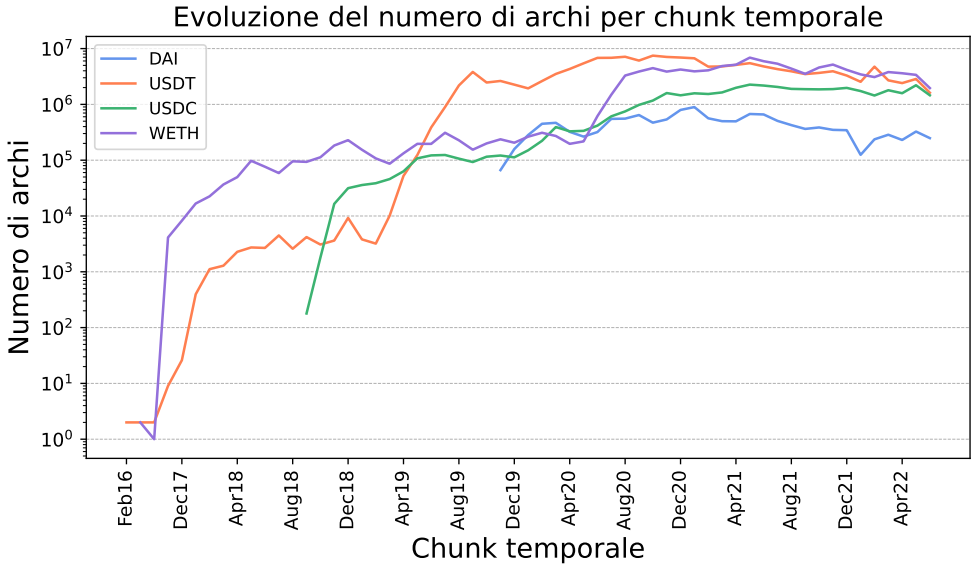


Figura 6.2: Evoluzione del numero di archi per ogni token.

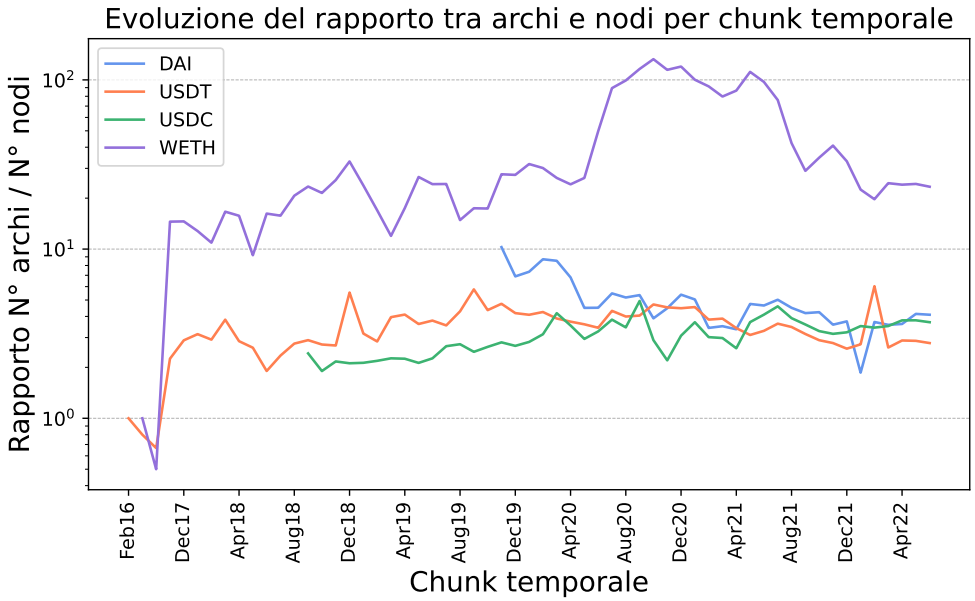


Figura 6.3: Evoluzione del numero di nodi per ogni token.

Questo conferma che le stablecoin come USDT e USDC sono frequentemente utilizzate come riserve di valore e strumento di scambio durante fasi di incertezza, mentre DAI e WETH mantengono un ruolo centrale nelle applicazioni DeFi [69].

Dall'evoluzione del rapporto tra numero di archi e numero di nodi in Figura 6.3, emerge chiaramente che WETH presenta un valore significativamente più elevato rispetto alle stablecoin. Questo comportamento suggerisce che, pur in presenza di un numero relativamente basso di nodi, WETH mantiene un numero di archi estremamente elevato. Ciò indica una rete caratterizzata da transazioni frequenti tra gli stessi nodi, riflettendo una struttura densa e concentrata. Questo fenomeno è coerente con il ruolo di WETH nelle DApps e nei protocolli DeFi, dove è preferito per la sua conformità allo standard ERC-20 e per la sua funzione di "*wrapped asset*", che ne facilita l'integrazione con smart contract e piattaforme decentralizzate. L'elevato rapporto tra archi e nodi suggerisce una possibile alta reciprocità, dove i nodi tornano frequentemente a scambiarsi valore nel tempo. Approfondiremo queste interazioni cicliche nella sezione successiva sulla reciprocità.

6.2.2 Reciprocità

La Figura 6.4 mostra che la reciprocità di WETH rimane significativamente più alta rispetto agli altri token durante tutto il periodo analizzato.

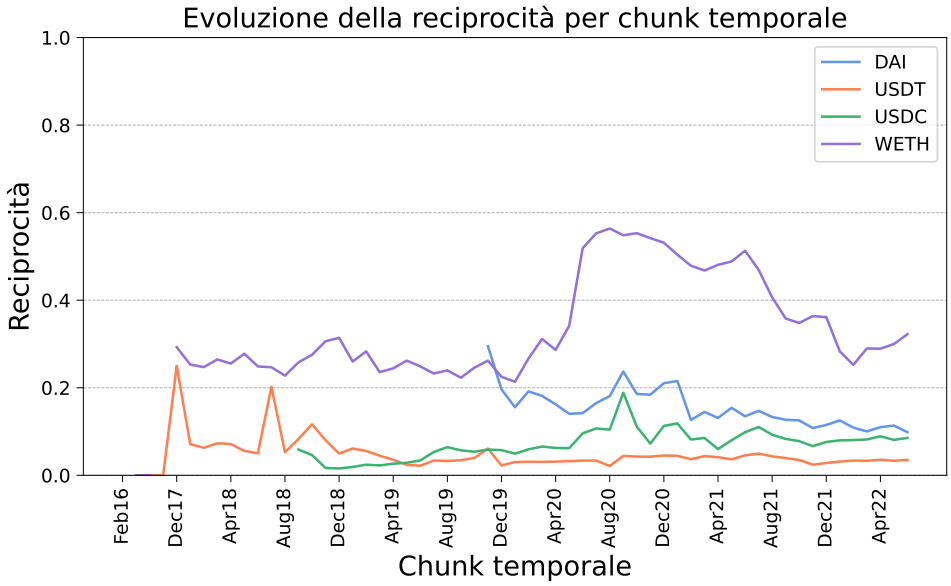


Figura 6.4: Evoluzione della reciprocità per ogni token.

Questo fenomeno riflette una rete in cui le transazioni cicliche, come depositi e prelievi frequenti, dominano l'interazione tra gli utenti. Come detto nella Sezione 6.2.1, questo fenomeno potrebbe essere spiegato dall'utilizzo di WETH nell'ambito di protocolli di lending/borrowing come Aave e Compound. Questi operano come

pool di liquidità aperti in cui gli utenti interagiscono come *lender (prestatori)* o *borrower (debitori)* senza la necessità di intermediari centralizzati. L'utilizzo di WETH come collaterale nei protocolli DeFi genera una dinamica di scambio continuo: i debitori depositano il token per ottenere prestiti in altri asset (ad esempio DAI o altre stablecoin) e, successivamente, ritirano il loro collaterale dopo aver saldato i prestiti.

Questo ciclo di *lending/borrowing* contribuisce all'aumento della reciprocità delle transazioni, poiché gli stessi nodi interagiscono ciclicamente per spostare o mantenere la liquidità. DAI presenta un comportamento intermedio: la reciprocità è maggiore rispetto a USDT e USDC, ma rimane inferiore a quella di WETH. Questo è attruibile al fatto che anche DAI potrebbe essere usato come collaterale in protocolli lending/borrowing. Al contrario, USDT e USDC mostrano livelli di reciprocità più bassi e stabili nel tempo. Ciò è dovuto principalmente al loro utilizzo prevalentemente come mezzi di pagamento e conservazione del valore, non influendo sulla reciprocità.

6.2.3 Distribuzioni gradi e forza: power law

L'analisi delle distribuzioni dei gradi in ingresso e in uscita per le reti di ciascun token (Istogrammi (a) e (b) delle Figure 6.5, 6.6, 6.7 e 6.8) rileva alcune caratteristiche interessanti ma non del tutto conformi a una distribuzione power law.

A questo proposito, le Tabelle 6.3a e 6.3b riportano i risultati del test statistico di Kolmogorov-Smirnov eseguito sui multigrafi globali tramite la libreria `plfit`, la qual valuta l'aderenza delle distribuzioni dei gradi a un modello di power law. Come indicato dai risultati del test, il `p-value` per tutte le distribuzioni è pari a 0. Secondo il riferimento teorico [55], un `p-value` maggiore di 0.1 è necessario per confermare che i dati seguano realmente una distribuzione power law. Il risultato del test per le nostre distribuzioni dei gradi suggerisce invece che queste reti non si conformano completamente a una tale distribuzione, nonostante i grafici mostrino una forma visivamente simile. Questo evidenzia la necessità di distinguere tra la conformità visiva e quella statistica, soprattutto quando si analizzano reti complesse come ERC-20.

Come evidenziato dalle tabelle, la libreria `plfit` ha fornito, oltre ai `p-value` , anche altre informazioni circa la distribuzione power law. In particolare, lo strumento utilizzato ha restituito anche l'esponente della power law (Alpha), il più piccolo valore per cui il fitting risulta valido (Xmin), la log-likelihood dei parametri (L) e l'errore di fitting (D), ovvero la distanza fra la distribuzione ottenuta mediante fitting e i dati in ingresso.

Tuttavia, considerati i `p-value` ottenuti per le quattro reti, la significatività di tali parametri risulta nulla. Ciò nonostante, si può sempre osservare come il valore di Alpha per WETH sia inferiore a quello delle stablecoin, il che riflette

una natura densa e focalizzata della rete di WETH. Al contrario, USDT e USDC mostrano valori di Alpha più alti e simili tra loro, riflettendo una distribuzione delle connessioni più ampia e meno concentrata. L'elevato volume transazionale di queste stablecoin riflette il loro impiego predominante come riserve di valore e strumenti di pagamento. Questo comportamento differisce in modo netto da quello di WETH, integrandole in reti più distribuite e meno centralizzate.

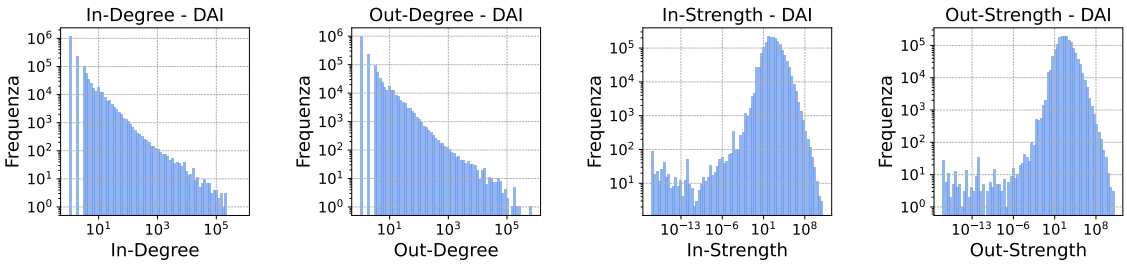
Token	InAlpha	InXmin	InL	InD	InPvalue
DAI	2.10104	4	-717249	0.00457181	0
USDT	2.19808	33	-1.92762e+06	0.00403033	0
USDC	2.22883	9	-1.20459e+06	0.00710627	0
WETH	1.70035	2	-1.45144e+06	0.00689161	0

(a) Statistiche distribuzioni gradi in ingresso

Token	OutAlpha	OutXmin	OutL	OutD	OutPvalue
DAI	2.06389	2	-1.29536e+06	0.00191343	0
USDT	2.12961	23	-2.10608e+06	0.00418745	0
USDC	2.25004	12	-886452	0.00811153	0
WETH	1.76361	2	-1.57817e+06	0.012886	0

(b) Statistiche distribuzioni gradi in uscita

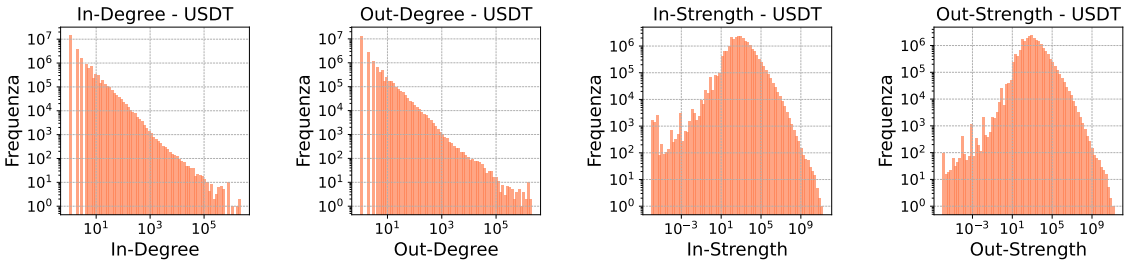
Tabella 6.3: Statistiche power law per ciascun token nei grafi globali tramite plfit (Sezione 5.2).



(a) (b) (c) (d)

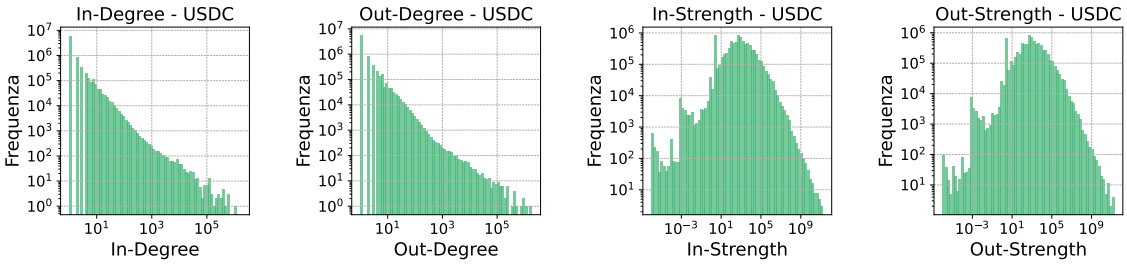
Figura 6.5: Distribuzioni gradi e forza in entrambe le direzioni per DAI.

Gli istogrammi (c) e (d) delle Figure 6.5, 6.6, 6.7 e 6.8, mostrano le distribuzioni della forza (o strength), ovvero il grado pesato sulla base della quantità di token trasferiti. Si nota che WETH ha valori di *in-strength* (forza in entrata) e *out-strength* (forza in uscita) elevati, concentrati su pochi nodi. Ciò indica che, oltre a effettuare molte transazioni, pochi nodi centrali gestiscono volumi di valore molto elevato. Al



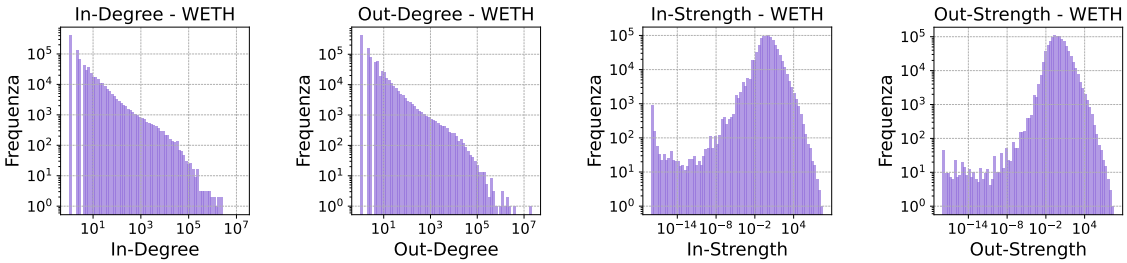
(a) (b) (c) (d)

Figura 6.6: Distribuzioni gradi e forza in entrambe le direzioni per USDT.



(a) (b) (c) (d)

Figura 6.7: Distribuzioni gradi e forza in entrambe le direzioni per USDC.



(a) (b) (c) (d)

Figura 6.8: Distribuzioni gradi e forza in entrambe le direzioni per WETH.

contrario, le stablecoin mostrano distribuzioni di forza più diffuse, coerenti con un utilizzo orientato a scambi regolari.

Oltre a queste analisi, è stato eseguito anche il test di conformità a una power law tramite `plfit` per ogni grafo temporale, ottenendo la stessa tipologia di risultati calcolati per il multigrafo globale descritti nelle Tabelle 6.3a e 6.3b. Dalle Figure 6.9 e 6.10 notiamo che, per il token DAI, il `p-value` rimane stabilmente sotto la soglia critica per la maggior parte dei chunk temporali. Questo suggerisce che la maggior

parte delle sottoreti temporali di DAI non seguono una distribuzione power law, in linea con i risultati globali dove il `p-value` ottenuto è 0.

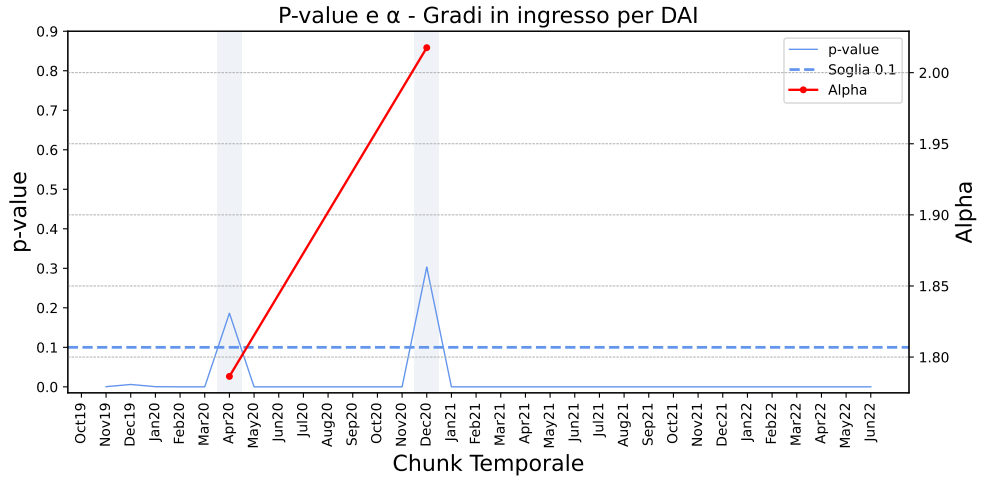


Figura 6.9: Andamento del `p-value` e α nel tempo per distribuzioni dei gradi in ingresso per DAI.

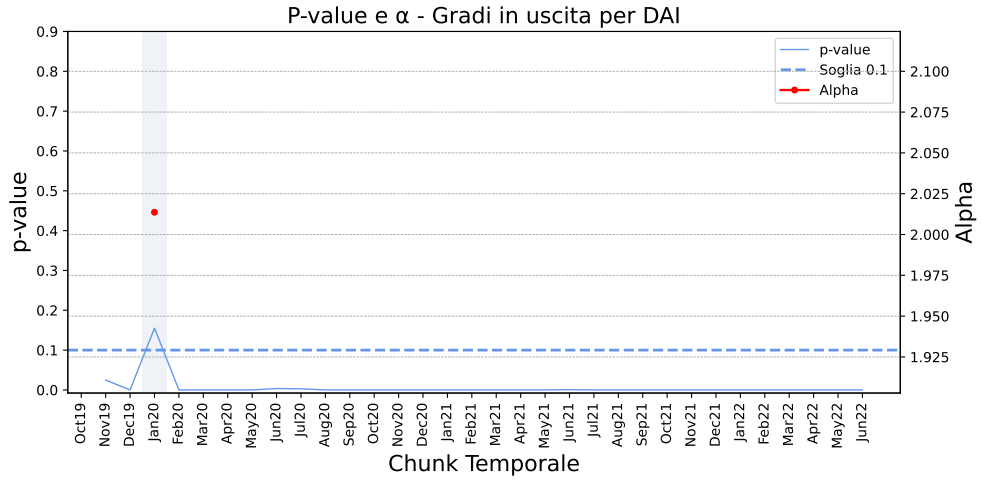


Figura 6.10: Andamento del `p-value` e α nel tempo per distribuzioni dei gradi in uscita per DAI.

Nelle Figure 6.11, 6.12, 6.13, e 6.14 mostriamo l'andamento per USDT e USDC dei `p-value` dei gradi in ingresso e in uscita. Entrambi i token mostrano `p-value` bassi (ovvero < 0.1), indicando che le distribuzioni dei gradi non seguono una power law. USDT presenta una serie di sottoreti temporali nel periodo iniziale che seguono

una power law. Al contrario, USDC presenta una rete più omogenea nel tempo data la sua scarsa aderenza ad una power law. In entrambi i casi, e analogamente a quanto visto nel caso di DAI, i risultati sono comunque conformi con quelli globali dove i `p-value` sono nulli.

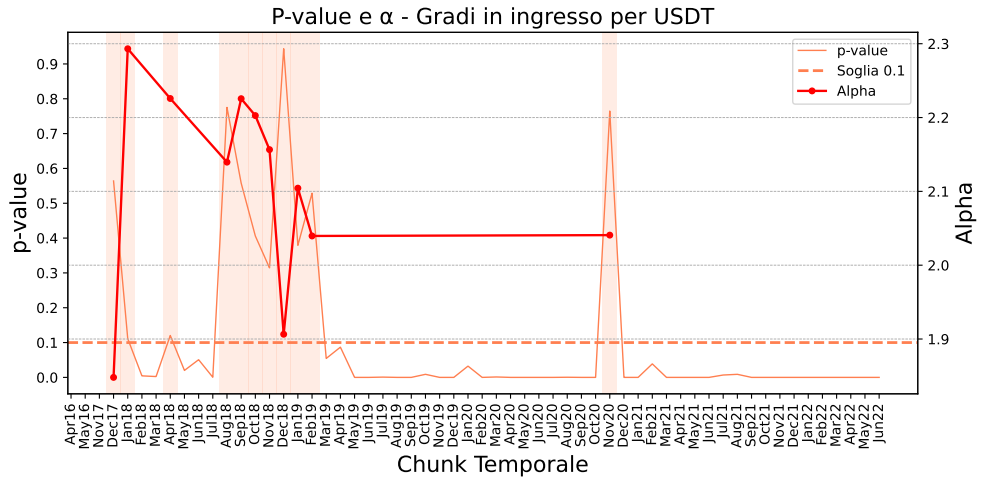


Figura 6.11: Andamento del `p-value` e α nel tempo per distribuzioni dei gradi in ingresso per USDT.

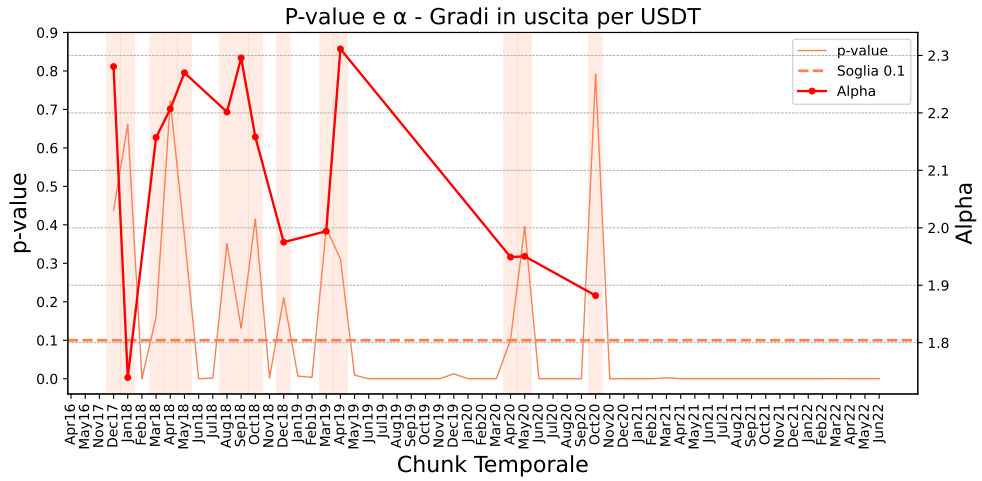


Figura 6.12: Andamento del `p-value` e α nel tempo per distribuzioni dei gradi in uscita per USDT.

Nelle Figure 6.15 e 6.16 mostriamo invece il caso di WETH. Questo è il token che più frequentemente presenta `p-value` superiori alla soglia critica dello 0.1, indicando

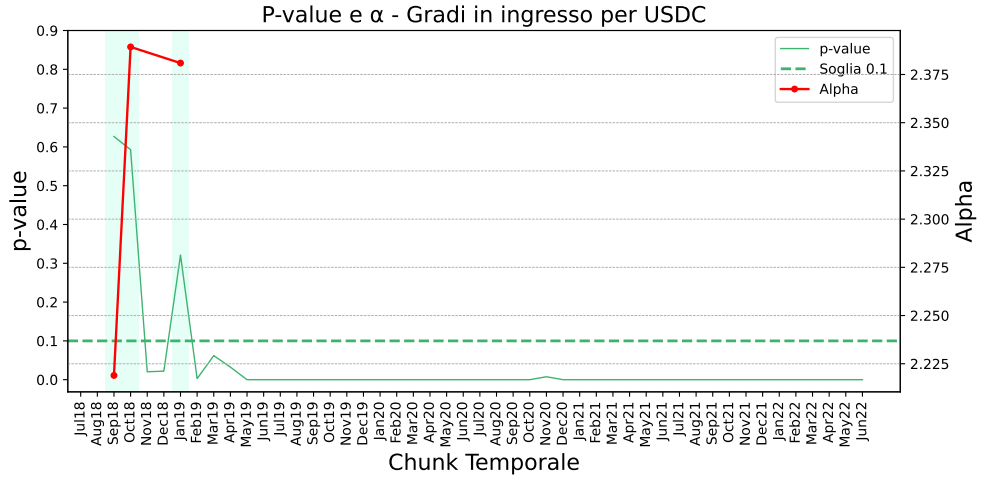


Figura 6.13: Andamento del `p-value` e α nel tempo per distribuzioni dei gradi in ingresso per USDC.

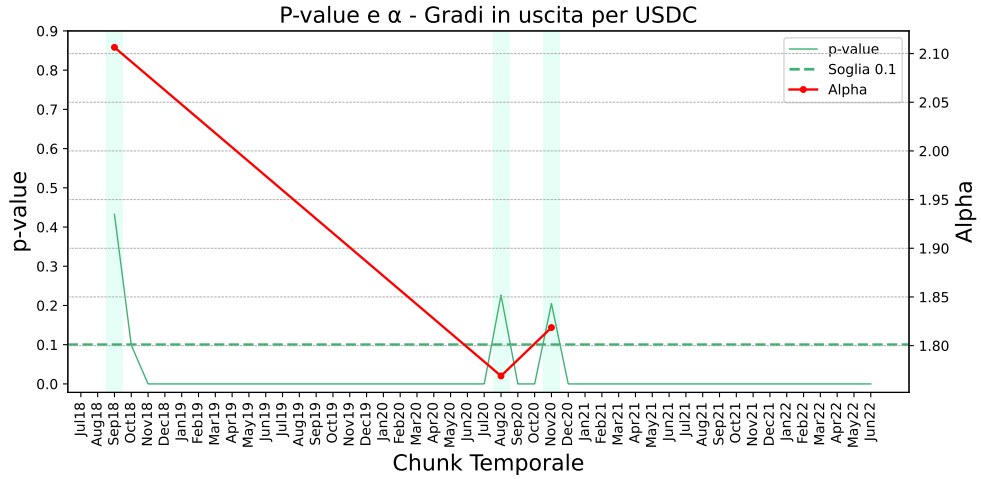


Figura 6.14: Andamento del `p-value` e α nel tempo per distribuzioni dei gradi in uscita per USDC.

che più volte la rete nel tempo segue effettivamente una power law. Tuttavia, è importante sottolineare che, nonostante questa conformità temporale, il grafo globale non soddisfa i requisiti statistici per una power law. Inoltre, come vedremo nella Sezione 6.2.5, WETH tende a formare più sottoreti fortemente connesse, fatto che sembrerebbe suggerire una frammentazione della rete globale. Questa configurazione lascia intendere che le interazioni transazionali si concentrano in cluster specifici, dominati da smart contract e pool di liquidità, piuttosto che distribuirsi uniformemente sull'intera rete, come invece avviene per le stablecoin. Tale comportamento

può spiegare perché, in alcuni chunk temporali, WETH mostra una maggiore tendenza a seguire una distribuzione power law dove la presenza dei cluster specializzati favorisce la formazioni di pochi nodi altamente connessi, nonostante il grafo globale non rispetti formalmente questo modello statistico.

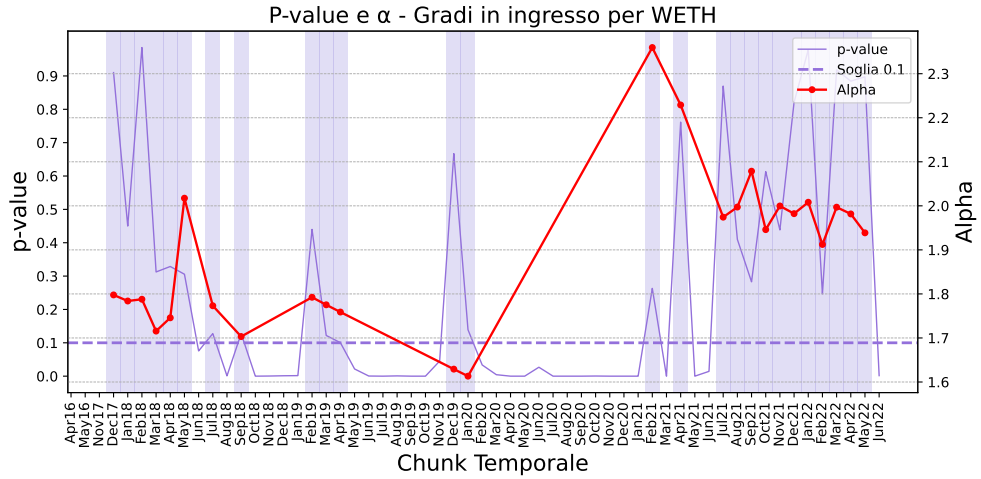


Figura 6.15: Andamento del `p-value` e α nel tempo per distribuzioni dei gradi in ingresso per WETH.

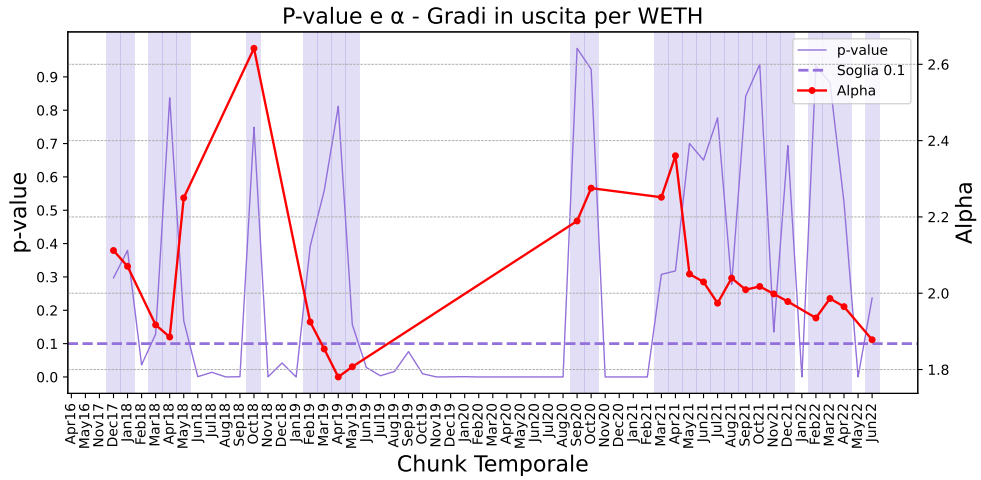
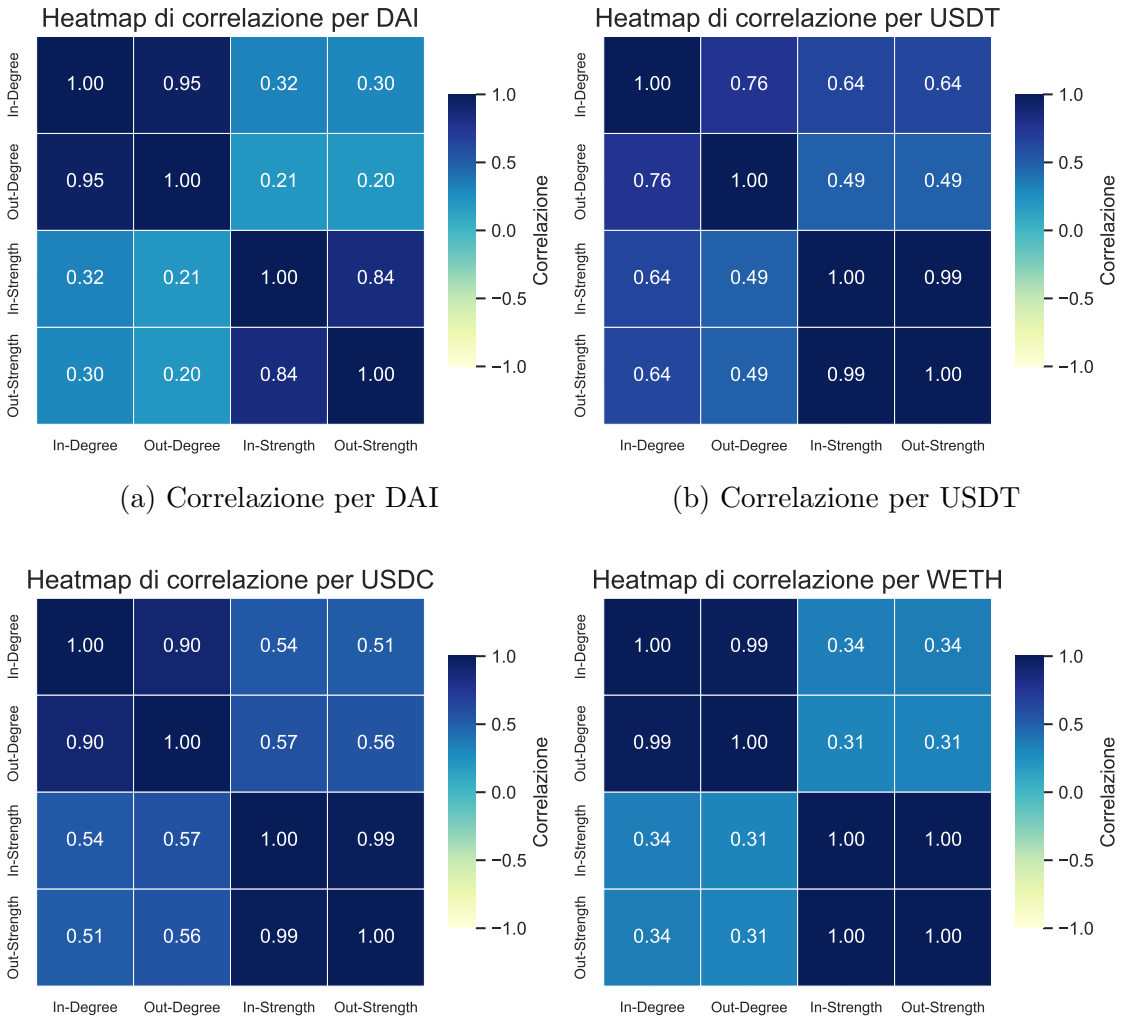


Figura 6.16: Andamento del `p-value` e α nel tempo per distribuzioni dei gradi in uscita per WETH.

6.2.4 Correlazioni tra metriche di rete

Le heatmap di correlazione delle metriche di rete per i quattro token, illustrate nella Figura 6.17, offrono una panoramica chiara e dettagliata delle relazioni tra il numero di connessioni (gradi in ingresso e in uscita) e i volumi delle transazioni (forze in ingresso e in uscita). Questi grafici permettono di comprendere come l'attività transazionale e la distribuzione del valore si differenziano tra i token analizzati, riflettendo i rispettivi contesti di utilizzo.



(a) Correlazione per DAI

(b) Correlazione per USDT

(c) Correlazione per USDC

(d) Correlazione per WETH

Figura 6.17: Heatmap di correlazione tra gradi e forze, in ingresso e in uscita, per ogni token.

Dalle Figure 6.17a e 6.17d emergono interessanti somiglianze tra DAI e WETH,

nonostante questi due token operino in contesti differenti. Entrambi presentano una correlazione molto alta tra *in-degree* (grado in ingresso) e *out-degree* (grado in uscita), suggerendo che i nodi tendono a bilanciare il numero di connessioni ricevute e inviate. Questo comportamento però non è esclusivo di DAI e WETH, ma è comune anche da altri token come USDC (Figura 6.17c), mentre USDT (Figura 6.17b) mostra una correlazione leggermente più bassa. Questo pattern generale riflette la natura intrinseca delle reti blockchain e del loro utilizzo nei protocolli DeFi. Questo evidenzia che sia nodi destinatari che mittenti di transazioni operano frequentemente, riflettendo il comportamento bilanciato che emerge dall'interazione ricorrente tra wallet, exchange e smart contract. Per WETH questo pattern è coerente con il fatto che viene largamente utilizzato per transazioni bidirezionali come swap e trasferimenti in pool di liquidità, incentivando un'alta reciprocità tra i nodi.

Tuttavia le correlazioni tra gradi e forze, ad esempio tra in-degree e in-strength, risultano deboli. Questo evidenzia la non proporzionalità tra il numero di connessioni e i volumi transazionali gestiti dai nodi, sottolineando che nodi altamente connessi non sono necessariamente responsabili di volumi elevati. Tale comportamento è particolarmente evidente dove pochi nodi centrali gestiscono un'alta concentrazione di valore, mentre altri partecipanti rimangono marginali, tipico nelle reti transazionali. In altre parole, un nodo molto attivo, che effettua molte transazioni, non è necessariamente un nodo "*ricco*", in termini di volumi di token gestiti. Questo ci porta a concludere che l'attività nella rete non è direttamente correlata alla ricchezza.

6.2.5 Copertura delle componenti connesse più grandi

La copertura delle componenti connesse rappresenta un aspetto cruciale per analizzare la struttura globale delle reti dei token ERC-20. Per copertura WCC (risp. SCC) intendiamo il rapporto fra il numero di nodi contenuti nella componente debolmente (risp. fortemente) connessa più grande e il numero complessivo di nodi nel grafo. La copertura WCC misura quanto la rete sia connessa globalmente, includendo percorsi unidirezionali, mentre quella relativa alla SCC quantifica la proporzione di nodi che possono comunicare tra loro tramite percorsi bidirezionali, fornendo informazioni sull'integrazione locale e sulle dinamiche reciproche.

Token	Copertura SCC	Copertura WCC
DAI	0.828552	0.998839
USDT	0.876751	0.999986
USDC	0.866046	0.999985
WETH	0.433595	0.975073

Tabella 6.4: Copertura delle SCC e WCC più grandi della rete globale del token.

I risultati globali, riportati nella Tabella 6.4, e i grafici delle evoluzioni temporali (Figura 6.18), evidenziano alcune caratteristiche distintive per i token analizzati. Le coperture WCC mostrano valori prossimi al 100% per le stablecoin e circa il 97.5% per WETH. Questo risultato evidenzia che quasi tutti i nodi, indipendentemente dal token, sono collegati tramite percorsi unidirezionali, formando una rete globalmente connessa. Le coperture SCC mostrano una differenza significativa tra WETH e le stablecoin; per queste ultime, la copertura varia tra l'82% e l'87%, mentre per WETH è notevolmente inferiore, attestandosi al 43.4%. Le stablecoin tendono a creare una singola componente fortemente connessa, che collega una vasta base di utenti tenendo conto della direzione degli archi. Al contrario, in WETH, che mostra una reciprocità significativamente alta, molte interazioni si concentrano in sottoreti ristrette e specializzate. Tali sottoreti limitano l'estensione della componente fortemente connessa globale e portano a un valore complessivo più basso rispetto alle stablecoin.

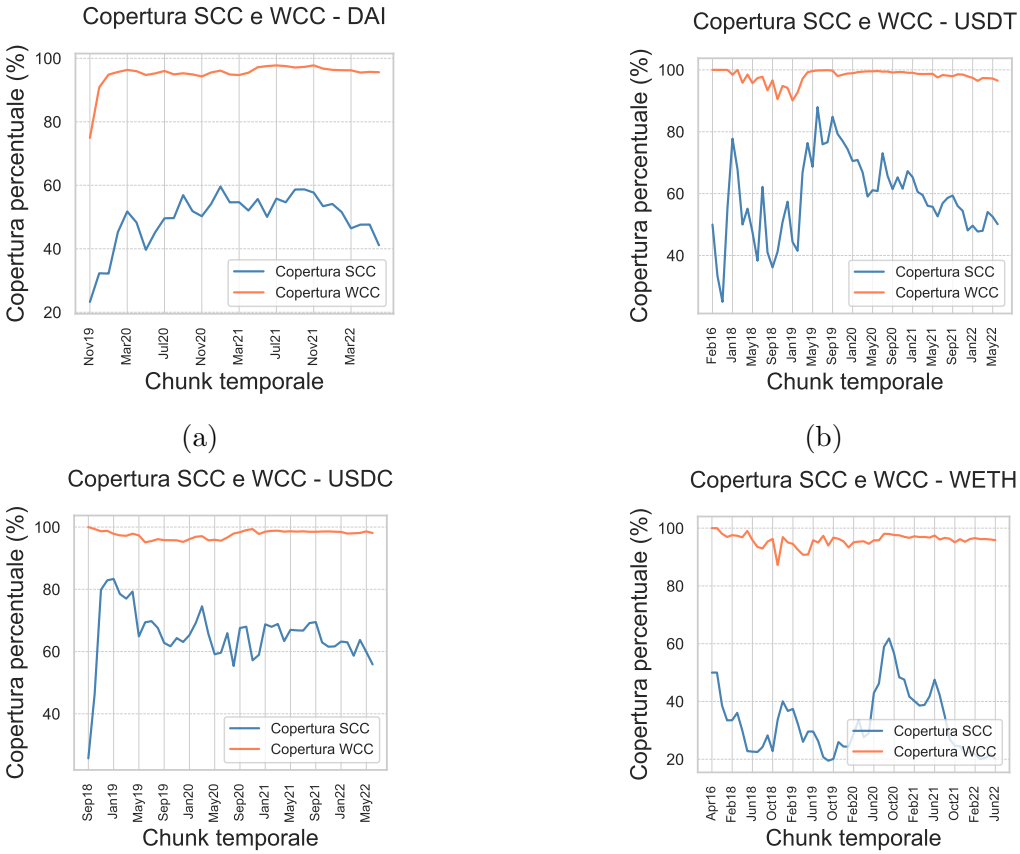


Figura 6.18: Evoluzioni della copertura delle SCC e WCC di ciascun token.

In Figura 6.18 è possibile osservare l'evoluzione della copertura WCC e SCC per ciascun token analizzato. In particolare, ricordiamo che nel corso della sua storia, Tether (USDT) (Grafico 6.18b) ha affrontato periodi di instabilità legati a controversie sulla trasparenza delle sue riserve (Sezione 3.3.1). Queste criticità potrebbero aver temporaneamente ridotto la fiducia degli utenti per USDT provocando un piccolo declino di interazione tra wallet e grandi exchange o smart contract, diminuendo la connettività [70]. Nonostante ciò, USDT è riuscito a mantenere una rete fortemente integrata, confermandosi come prima stablecoin sul mercato. Diversamente, DAI presenta un'adozione inizialmente più graduale (Figura 6.18a), riflessa nei valori bassi di copertura SCC e WCC nelle prime fasi temporali. WETH, pur mostrando una copertura WCC elevata fin dalle prime fasi (Figura 6.18d), presenta una copertura SCC significativamente più bassa rispetto alle stablecoin. Questo riflette una rete meno distribuita e più concentrata, in cui le interazioni sono limitate a cluster ristretti dominati da pochi nodi principali, come smart contract ed exchange. La natura di WETH come collaterale e mezzo di scambio in protocolli DeFi, come Aave e Uniswap, favorisce transazioni bidirezionali all'interno di questi cluster. Tuttavia queste interazioni rimangono circoscritte a sottoreti specifiche, facendo sì che, dal punto di vista della copertura SCC, la rete globale risulti più frammentata rispetto alle stablecoin.

6.2.6 Assortatività

L'analisi dell'assortatività rivela dinamiche fondamentali sulle preferenze di connessione nella rete di transazioni ERC-20. Dai risultati ottenuti illustrati in Figura 6.19, possiamo osservare che tutte le reti dei token mostrano un comportamento *disassortativo*, ovvero hanno valori negativi di assortatività. Questo implica che i nodi con molte connessioni (detti hub) tendono a connettersi con nodi meno connessi.

Questo è un risultato atteso dati i risultati descritti finora: infatti, pur non seguendo una distribuzione power law, le distribuzioni dei gradi e delle forze mostrano la presenza di nodi centrali che gestiscono grandi volumi di transazioni. Nel caso delle stablecoin fiat-collateralizzate come USDT e USDC, questa disassortatività è particolarmente marcata. I nodi centrali potrebbero infatti corrispondere agli exchange, i quali gestiscono grandi volumi di transazioni da e verso un'ampia base di utenti periferici. In questi casi le reti sono fortemente "polarizzate", dove pochi hub sono coinvolti nella maggior parte delle transazioni. Per quanto riguarda WETH, i suoi valori di assortatività, sia per grado che per forza (in ingresso e in uscita), sono meno estremi rispetto a quelli osservati per le stablecoin fiat, come USDT e USDC. Questo suggerisce che la rete di WETH ha una maggiore tendenza a collegare nodi con caratteristiche simili, pur mantenendo un comportamento generale disassortativo. Infine, DAI rappresenta un caso intermedio fra le stablecoin collateralizzate fiat e WETH. Sebbene nelle analisi precedenti DAI abbia mostrato somiglianze con

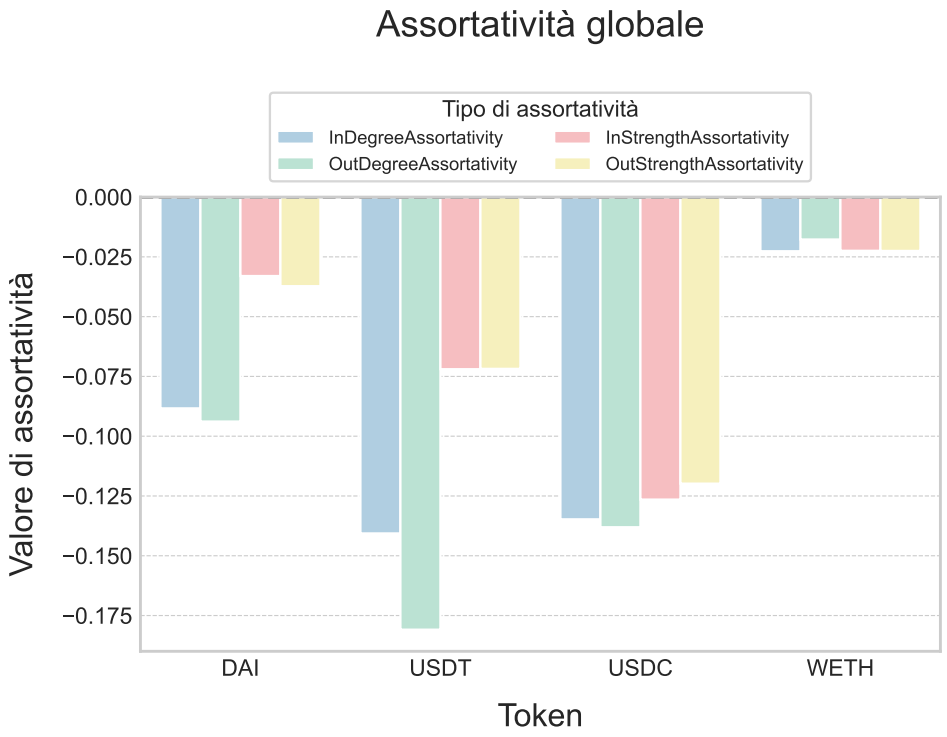


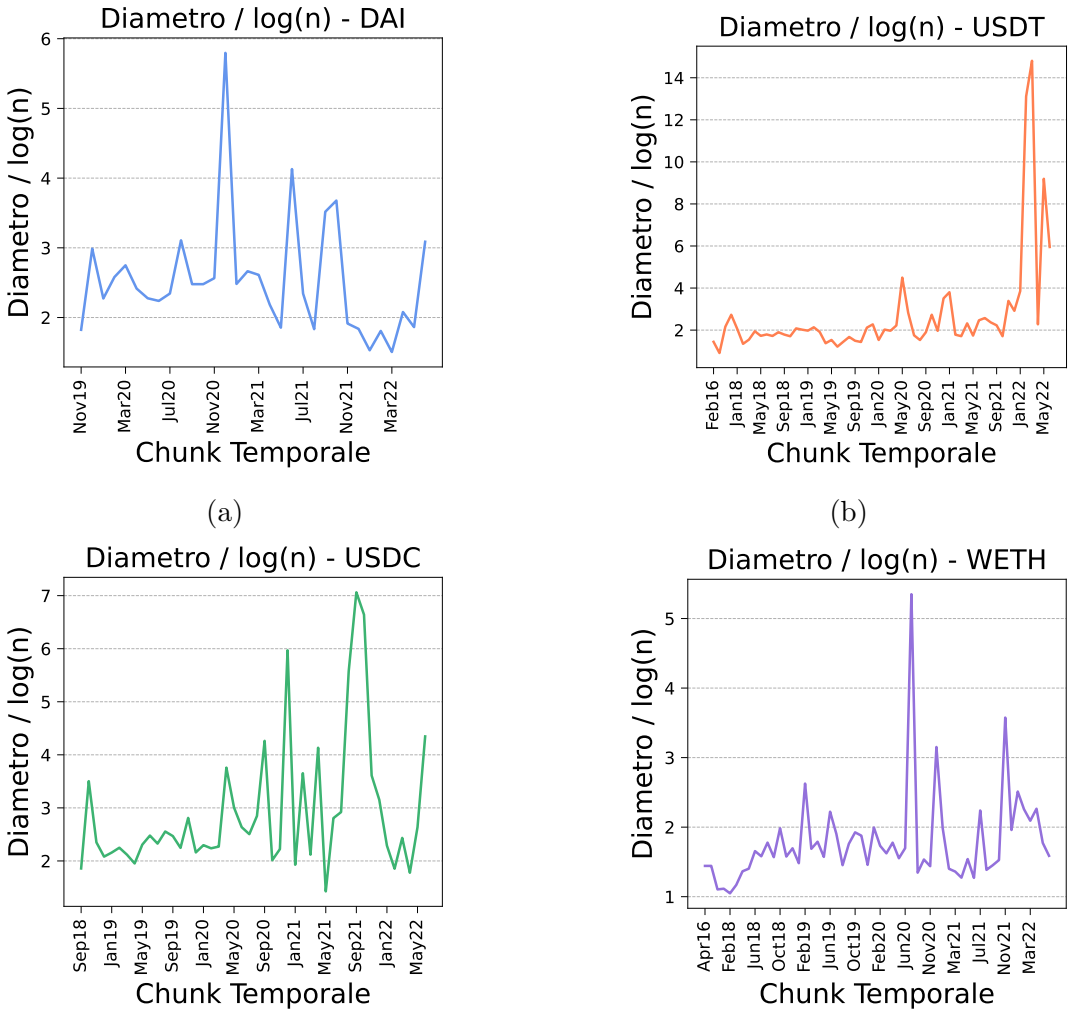
Figura 6.19: Assortatività di grado e di forza per entrambe le direzioni di ogni token.

WETH, in questo caso le sue metriche di assortatività risultano più vicine a quelle delle stablecoin fiat.

6.2.7 Diametro e coefficiente di clustering

Per approfondire ulteriormente il livello di coesione della rete, abbiamo analizzato anche il diametro relativo, ovvero il rapporto fra il diametro e il logaritmo del numero dei nodi della rete. I valori osservati per il diametro relativo sottolineano l'efficienza con cui le reti consentono la trasmissione di valore. Dalle Figure 6.20a e 6.20d, si può notare come per DAI e WETH il diametro relativo rimanga basso e stabile nel corso del tempo. Questo comportamento è coerente con le proprietà osservate nelle reti small-world, che combinano percorsi brevi con un'elevata coesione locale. Tuttavia, è importante precisare che il basso diametro relativo è una condizione necessaria, ma non sufficiente, per classificare una rete come small-world. Tali reti infatti richiedono anche un elevato coefficiente di clustering, valore che sarà analizzato più avanti nel corso di questa sezione. Osservando invece le Figure 6.20b e 6.20c, possiamo dedurre che USDT e USDC mostrano una maggiore variabilità nel diametro relativo, con picchi che riflettono una frammentazione temporanea della rete, anche se la media

rimane abbastanza stabile e bassa. Nonostante queste variazioni, il diametro basso suggerisce che tutte le reti analizzate condividano alcune somiglianze con le small-world, con percorsi brevi e un'efficiente connessione globale. Tuttavia, come detto precedentemente, l'analisi del coefficiente di clustering risulta cruciale per rivelare se queste reti possiedono la coesione locale necessaria per essere classificate come tali.



(a) (b) (c) (d)

Figura 6.20: Evoluzione del diametro relativo per ogni token.

Dall'analisi dell'evoluzione del coefficiente di clustering (o transitività) riportata nella Figura 6.21, emerge che le reti dei token ERC-20 presentano valori generalmente bassi per questa metrica. In particolare, DAI mostra un coefficiente di clustering

relativamente stabile nel tempo. WETH, al contrario, evidenzia un trend in crescita, suggerendo un'espansione delle connessioni localizzate nel tempo. Infine, le stablecoin fiat-collateralizzate, ovvero USDT e USDC, mostrano valori di clustering significativamente inferiori rispetto a DAI e WETH, con una dinamica temporale relativamente stabile. Questo risultato è coerente con la loro funzione primaria di trasferimento di valore e pagamenti unidirezionali, dove le connessioni tra i nodi sono distribuite in maniera più uniforme, senza concentrazioni significative attorno a cluster locali.

Tuttavia, i valori assoluti rimangono troppo bassi per classificare le quattro reti come small-world, nonostante il diametro relativo basso. Questo comportamento riflette una progettazione orientata all'efficienza nella trasmissione del valore verso i nodi principali, piuttosto che alla formazione di cluster locali coesi. Tali risultati sono coerenti con lo studio [71], che sottolinea l'importanza del clustering per definire le proprietà small-world.

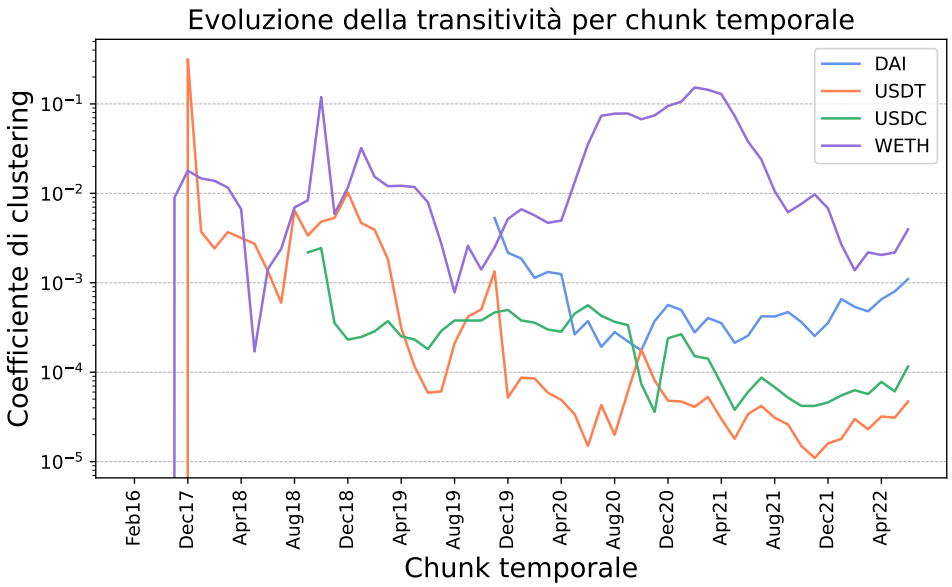


Figura 6.21: Evoluzione della transitività (coefficiente di clustering) per ogni token.

6.2.8 Densità della rete

Analizzando l'evoluzione della densità possiamo trarre delle conclusioni importanti sulle diverse reti analizzate, soprattutto per WETH.

Dalla Figura 6.22 notiamo che all'inizio del periodo analizzato, le reti ERC-20 dei token mostrano valori di densità relativamente più alti, conforme con le fasi iniziali delle reti blockchain, quando il numero di nodi è ridotto e le connessioni

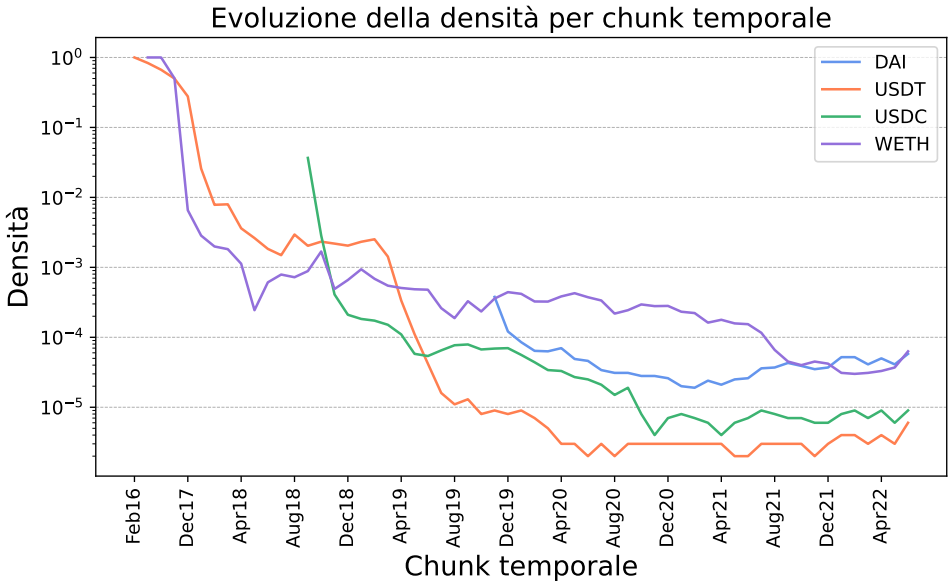


Figura 6.22: Evoluzione della densità per ogni token.

sono concentrate tra un numero limitato di attori principali. Con il passare del tempo, però, la densità diminuisce e si stabilizza, riflettendo l'espansione della rete e una maggiore distribuzione delle interazioni tra i nodi.

In particolare per WETH la densità più alta nel tempo è particolarmente significativa. Infatti, come discusso in precedenza nella Sezione 6.2.1, questo token viene utilizzato molto spesso per transazioni ricorrenti, spesso tra pochi nodi centrali. Questo comportamento è coerente con la sua alta reciprocità, che indica una rete densa localmente ma meno distribuita globalmente rispetto ai token stablecoin. Tuttavia la densità assoluta rimane molto bassa, fatto che sembra giustificare come in queste reti nodi "comuni" che rappresentano la maggioranza di attori della rete, ovvero wallet individuali, si connettono raramente tra di loro, costruendo quindi una rete con flusso maggiore sui pochi nodi centrali.

6.3 Analisi delle centralità

Le metriche di centralità rappresentano strumenti fondamentali per analizzare il comportamento delle reti ERC-20, permettendo di identificare i nodi più rilevanti dal punto di vista economico e funzionale. In particolare, metriche come il PageRank, la harmonic centrality, l'hub e l'authority score consentono di studiare la distribuzione del valore e il ruolo di nodi chiave all'interno della rete. Queste misure sono cruciali per comprendere come il valore transazionale fluisce tra wallet,

exchange e smart contract, evidenziando non solo l'importanza globale di un nodo, ma anche la sua posizione nei cluster locali e il suo ruolo specifico nella rete. Per una descrizione approfondita dei principi teorici e degli algoritmi utilizzati per calcolare queste metriche, si rimanda alle Sezioni 5.9, 5.11 e 5.10.

6.3.1 Distribuzione delle centralità per token

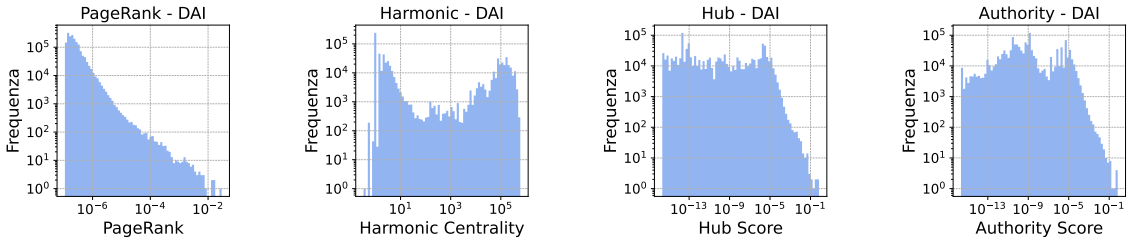
Come prima analisi, abbiamo calcolato le quattro misure di centralità (PageRank, harmonic centrality, Hub e Authority score) per ciascun nodo all'interno delle reti globali. Come evidenziato dalle Figure 6.23, 6.24, 6.25 e 6.26, le distribuzioni delle metriche di centralità presentano caratteristiche specifiche che riflettono la struttura e il funzionamento delle reti ERC-20 analizzate. In particolare osserviamo comportamenti omogenei per le stablecoin USDT, USDC e DAI, mentre WETH si distingue per un pattern più concentrato. Queste osservazioni sono coerenti con i ruoli economici e le strutture topologiche descritte nella Sezione 6.2.

Si noti che il PageRank è stato calcolato considerando come peso degli archi il numero di transazioni tra coppie di nodi (vedi Sezione 5.9). Le distribuzioni del PageRank per tutte le reti (Figure 6.23a, 6.24a, 6.25a e 6.26a) seguono un andamento decrescente, simile a una legge di potenza con una coda lunga. Questo pattern riflette una rete altamente eterogenea, dove pochi nodi "hub" ottengono un PageRank molto elevato, mentre la maggior parte dei nodi ha valori di PageRank relativamente bassi. Questo comportamento è coerente con la struttura tipica delle reti transazionali, caratterizzate da una concentrazione dell'attività su pochi nodi chiave. In generale, le distribuzioni sono simili tra loro, dove l'attività è dominata da pochi nodi principali: questo ci mostra come i nodi con un elevato nuemero di connessioni entranti, specialmente da nodi già autorevoli, tendono a emergere come hub centrali.

Le distribuzioni dell'harmonic centrality (Figure 6.23b, 6.24b, 6.25b e 6.26b) indicano che molti nodi della rete mantengono un buon livello di accessibilità, anche se non sono tra i più centrali. Questo suggerisce che, oltre ai nodi principali con alta centralità armonica, vi è un numero significativo di nodi con valori intermedi, che contribuiscono a mantenere percorsi relativamente brevi verso il resto della rete. Questo è conforme al diametro che segue il logaritmo del numero di nodi.

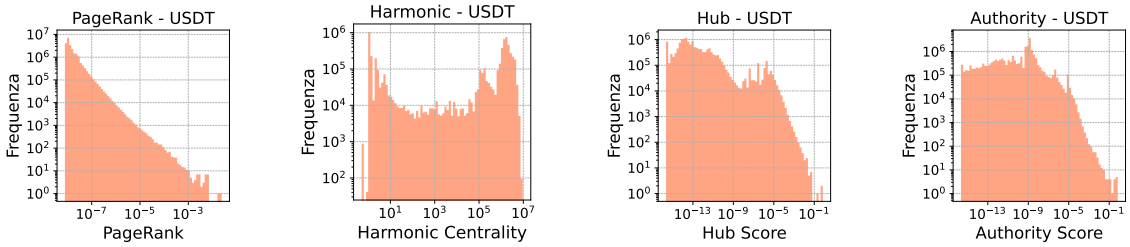
Infine, le distribuzioni di hub e authority score, illustrate dagli istogrammi (c) e (d) delle Figure 6.23, 6.24, 6.25 e 6.26, sembrano seguire pattern generali simili tra i diversi token, seppur con piccole variazioni. Per DAI sia gli hub che gli authority score mostrano una distribuzione relativamente uniforme: gli hub sono distribuiti su un numero maggiore di nodi, riflettendo una rete leggermente più decentralizzata rispetto ad altre stablecoin, mentre gli authority sono anch'essi più distribuiti, indicando che l'accumulo di transazioni non è dominato esclusivamente da pochi nodi centrali. USDT e USDC seguono un pattern simile ovvero: i due score decresco-

no rapidamente, con pochi nodi che concentrano la maggior parte delle connessioni che suggerisce che i nodi centrali fungono sia da hub che da punti di raccolta di transazioni per i due token. In WETH invece la distribuzione degli score è più uniforme, con una coda lunga più pronunciata dove numerosi nodi agiscono come hub e authority.



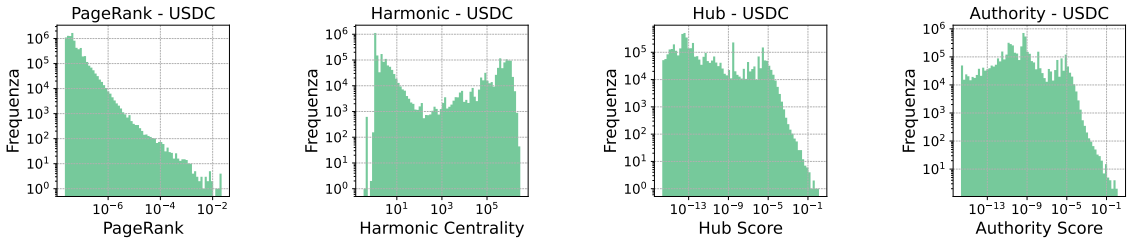
(a) (b) (c) (d)

Figura 6.23: Distribuzioni delle centralità per DAI.



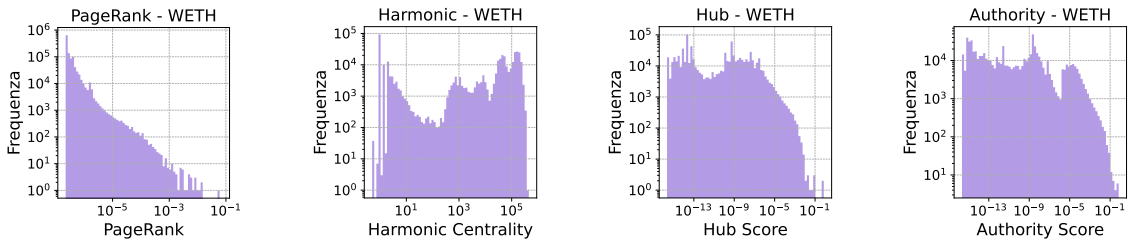
(a) (b) (c) (d)

Figura 6.24: Distribuzioni delle centralità per USDT.



(a) (b) (c) (d)

Figura 6.25: Distribuzioni delle centralità per USDC.



(a) (b) (c) (d)

Figura 6.26: Distribuzioni delle centralità per WETH.

6.3.2 Top 10 nodi per centralità

Individuare i nodi più centrali nelle reti dei token analizzati è stato fondamentale per comprendere le dinamiche strutturali delle reti stesse. Attraverso un'analisi combinata, sia globale che temporale, è stato possibile identificare non solo i nodi costantemente centrali, ma anche quelli che assumono una rilevanza particolare in specifici periodi di attività. Questo approccio ha permesso di spiegare perché le reti analizzate dei quattro token mostrano determinati comportamenti strutturali, come la formazione di hub, la concentrazione di transazioni su determinati nodi o la variazione della connettività nei periodi di maggiore o minore utilizzo. In questo modo, è stato possibile ottenere una visione più profonda del ruolo di questi nodi nell'organizzazione e nell'evoluzione complessiva delle reti, evidenziando le loro influenze sull'efficienza, la resilienza e l'adattabilità delle strutture globali.

Da ciascun grafo sono stati estratti i primi 100 nodi per ogni metrica di centralità, selezionati in base al punteggio ottenuto. Nei grafi globali, questi nodi rappresentano gli attori con la maggiore rilevanza complessiva, capaci di influenzare l'intera rete attraverso interazioni persistenti. Nei grafi temporali, invece, i top 100 nodi variano chunk per chunk, riflettendo dinamiche locali e temporanee. Il passo successivo è stato quello di recuperare gli indirizzi di tali nodi mappando l'identificativo numerico nell'hash corrispondente all'interno del dataset originale degli indirizzi ERC-20 (ovvero il file `erc20_addresses.csv.xz` presentato nella Sezione 6.1). Dopodiché abbiamo combinato le classifiche temporali per ciascuna metrica: per ognuna di esse, le top 100 relative ai diversi chunk temporali sono state unite per ottenere una lista di nodi unici. Questa unione ha permesso di aggregare tutti i nodi che, in almeno un chunk, sono stati classificati tra i primi 100 per una metrica di centralità. Ogni nodo nella lista è stato poi associato alla frequenza con cui appare nei chunk temporali per quella metrica stessa, o meglio quante volte un nodo si è classificato tra i primi 100 di quella centralità nei grafi temporali. Un nodo che compare frequentemente in queste classifiche dimostra una centralità stabile e ripetuta nel tempo, assumendo un ruolo strutturale importante per la rete. Al contrario, un nodo che appare

raramente o in un numero limitato di chunk può avere una centralità elevata solo in alcuni periodi specifici, legata ad eventi temporanei o attività occasionali. Successivamente, per ogni nodo della lista unificata, è stato verificato se fosse presente nella top 100 globale della metrica corrispondente. Ciò è stato fatto mediante un campo booleano che vale:

- `1` se il nodo è incluso nella top 100 globale di quella metrica.
- `0` se il nodo *non* è presente nella top 100 globale di quella metrica.

Questa verifica aggiuntiva consente di distinguere nodi che possiedono una rilevanza globale stabile da quelli che sono invece centrali solo in determinati periodi temporali. Ad esempio se un nodo appare frequentemente nei chunk temporali ma non nella top 100 globale potrebbe essere significativo per eventi specifici, mentre un nodo che compare in entrambe le classifiche dimostra una centralità strutturale su scala globale.

Infine, analizzando le loro occorrenze all'interno delle classifiche dei top 100 nei chunk temporali, abbiamo quindi selezionato i 10 nodi più frequenti per ciascun token e ciascuna metrica. Per comprendere al meglio il processo di selezione, nella Tabella 6.5 sono evidenziati i top 10 nodi relativamente a una singola misura di centralità e un solo token, nello specifico la centralità PageRank di USDT. I risultati completi vengono poi descritti in grafici a barre opportuni successivamente. La tabella rappresenta un esempio pratico del risultato dell'approccio adottato. Per ogni metrica di centralità, i top 10 nodi con la maggiore frequenza nei chunk temporali sono stati considerati come i più centrali, riflettendo una combinazione di rilevanza temporale e importanza globale.

Hash	PageRank	Hub	Authority	Harmonic	BPageRank	BHub	BAuthority	BHarmonic
0x0d...2fe	51	20	1	51	1	0	0	1
0x87...0fa	47	29	10	34	1	0	0	1
0x75...b88	38	4	0	36	1	0	0	0
0x67...f2b	35	15	0	40	1	0	0	1
0xfb...b98	35	4	0	31	1	0	0	0
0x10...ab3	34	17	1	39	1	0	0	1
0xab...24f	34	15	0	38	1	0	0	1
0xfd...0ad	33	14	0	36	1	0	0	1
0xc9...bc5	33	0	0	0	1	0	0	0
0x47...b6f	32	4	1	19	1	0	0	0

Tabella 6.5: Esempio di top 10 nodi per centralità PageRank per il token USDT.

Visualizzazione dei top 10 per centralità

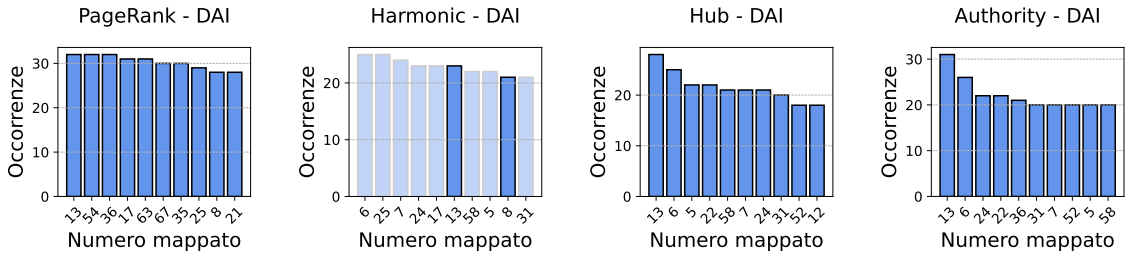
Per ogni nodo classificato tra i top 10 di una specifica metrica di centralità, è stato utilizzato il relativo indirizzo per effettuare uno "*scraping*" dalla piattaforma *Etherscan*, al fine di ottenere il nome reale associato al wallet o allo smart contract. Questo

passaggio è stato cruciale per identificare la natura dei nodi centrali, per distinguere exchange dai protocolli DeFi o wallet individuali. Successivamente per garantire una rappresentazione chiara e uniforme, ogni nome è stato mappato a un numero identificativo univoco all'interno di ciascuna top 10 locale di quella centralità. Ciò ha prodotto 16 tabelle distinte, ciascuna rappresentante i top 10 nodi di una metrica di centralità per un determinato token il che permette di confrontarle tra di loro e individuare eventuali sovrapposizioni o pattern comuni. L'obiettivo di questa analisi è confrontare i risultati sia tra le centralità di un singolo token sia tra i token stessi, individuando nodi molto centrali, ovvero coloro che compaiono ripetutamente nelle top 10 di più metriche per lo stesso token, e sia nodi "trasversali" ovvero coloro che risultano centrali in più token, mostrando un ruolo dominante su reti differenti.

Per presentare i risultati della nostra analisi, nei paragrafi successivi mostriamo una serie di grafici a barre che riassumono i 10 nodi più frequenti nei ranking di centralità per ogni metrica e per ogni token considerato. Inoltre, per mostrare se un nodo è compreso anche nella top 100 globale di quella metrica, le barre corrispondenti sono state rappresentate con un colore più acceso, mentre per i nodi non presenti nei ranking globali le barre risultano più sbiadite. Per illustrare l'identità dei nodi, infine, sotto ogni grafico è riportata una tabella riassuntiva che contiene l'associazione fra l'identificativo numerico del nodo e un'etichetta (ottenuta tramite scraping) con il nome dell'entità.

I risultati relativi ai nodi centrali di DAI (Figure 6.27 e 6.28) confermano quanto emerso dall'analisi strutturale e topologica della rete (vedi Sezione 6.2). Il ruolo di DAI come mezzo di scambio e riserva decentralizzata viene confermata dalla presenza predominante di nodi associati a piattaforme DeFi come *UniSwap*, *SushiSwap* e *Compound*, che fungono da fulcri per il flusso di valore. In particolare, *UniSwap V2* si distingue come uno dei nodi più rilevanti evidenziando la sua funzione nella gestione della liquidità e nell'aggregazione delle transazioni [72]. Nel contempo la presenza di nodi come *Compound* conferma l'utilizzo di DAI come asset collaterale nei protocolli di lending, dove viene costantemente depositato e prelevato da utenti che interagiscono con gli smart contract del protocollo. Questo spiega il motivo per cui questi nodi appaiono anche in metriche come hub score, riflettendo il ruolo attivo nel distribuire valore ad altri indirizzi. Inoltre l'apparizione di indirizzi "*anonimi*", come `0x56...bf9`, tra i nodi centrali suggerisce che la rete non è dominata esclusivamente da entità note o istituzionali. Un altro elemento interessante è la presenza di *MEV bot* tra i nodi più centrali di DAI. Questi bot giocano un ruolo fondamentale nei pool di liquidità, sfruttando opportunità di arbitraggio e ottimizzando la sincronizzazione dei prezzi tra i DEX [73]. La loro centralità è coerente con la natura dinamica della rete di DAI, dove i pool di liquidità sono soggetti a fluttuazioni rapide.

I nodi centrali individuati per USDT (Figure 6.29 e 6.30), risultano essere in par-



(a) (b) (c) (d)

Figura 6.27: Grafici a barre per i top 10 nodi per centralità del token DAI.

N°	Nome
13	0x56...bf9
54	Crypto.com
36	Compound: cDAI Token
17	Kraken 12
63	Forwarder Creator: 0xbf0...e4e
67	HitBTC 3
35	0xd3...2f6
25	Nexo 2
8	Crypto.com 2
21	Wirex 5

(a)

N°	Nome
6	UniSwap V2: DAI
25	Nexo 2
7	UniSwap V2: DAI/USDC
24	0x: Exchange Proxy Fl. Wal.
17	Kraken 12
13	0x56...bf9
58	UniSwap V2: DAI-USDT
5	SushiSwap: DAI
8	Crypto.com 2
31	MetaMask: Swaps Spender

(b)

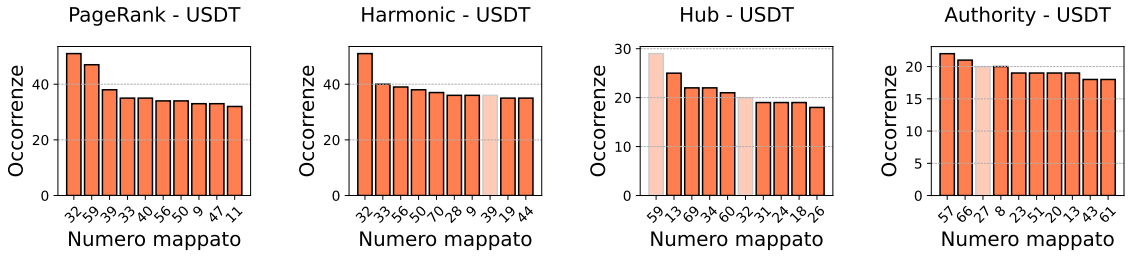
N°	Nome
13	0x56...bf9
6	UniSwap V2: DAI
5	SushiSwap: DAI
22	MEV Bot: 0xa57...6CF
58	UniSwap V2: DAI-USDT
7	UniSwap V2: DAI/USDC
24	0x: Exchange Proxy Fl. Wal.
31	MetaMask: Swaps Spender
52	MEV Bot: 0x000...f56
12	UniSwap: DAI

(c)

N°	Nome
13	0x56...bf9
6	UniSwap V2: DAI
24	0x: Exchange Proxy Fl. Wal.
22	MEV Bot: 0xa57...6CF
36	Compound: cDAI Token
31	MetaMask: Swaps Spender
7	UniSwap V2: DAI/USDC
52	MEV Bot: 0x000...f56
5	SushiSwap: DAI
58	UniSwap V2: DAI-USDT

(d)

Figura 6.28: Tabelle mapping (N°,Nome) del Grafico 6.27 - DAI.



(a) (b) (c) (d)

Figura 6.29: Grafici a barre per i top 10 nodi per centralità del token USDT.

N°	Nome
32	Gate.io 1
59	Bitfinex 3
39	MEXC 1
33	HTX 2
40	Bittrex
56	HTX 9
50	HTX 1
9	HTX 3
47	ZB.com 5
11	MainCoin 1

(a)

N°	Nome
32	Gate.io 1
33	HTX 2
56	HTX 9
50	HTX 1
70	HTX 12
28	HTX 7
9	HTX 3
39	MEXC 1
19	HTX 4
44	HTX 36

(b)

N°	Nome
59	Bitfinex 3
13	0x56...bf9
69	SushiSwap: USDT
34	UniSwap V2: USDT
60	Binance
32	Gate.io 1
31	MetaMask: Swaps Spender
24	0x: Exchange Proxy Fl. Wal.
18	Tokenlon: PMM
26	UniSwap V2: USDC-USDT

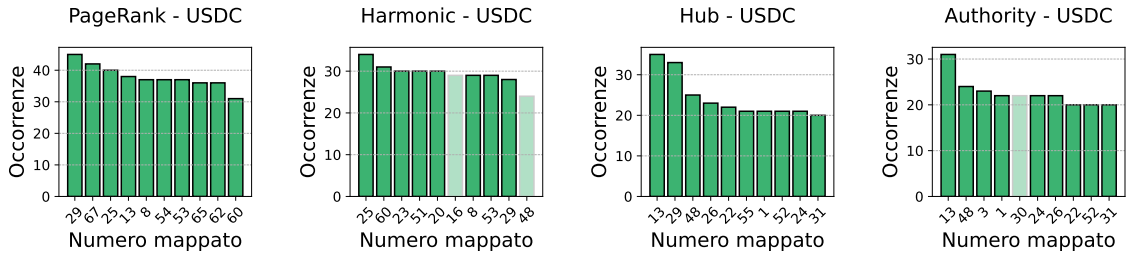
(c)

N°	Nome
57	HTX
66	Alemeda Research 5
27	0x75...2fe
8	Crypto.com 2
23	Binance 2
51	Binance 3
20	Binance 4
13	0x56...bf9
43	0xc3...771
61	0xb3...0aa

(d)

Figura 6.30: Tabelle mapping (N°,Nome) del Grafico 6.29 - USDT.

te diversi rispetto a quelli osservati per DAI ma riflettono la natura della stablecoin fiat-collateralizzata. La rete mostra infatti una maggiore concentrazione attorno a pochi nodi globalmente rilevanti. I nodi principali emersi come Bitfinex, Binance e HTX, agiscono come hub globali, attirando la maggioranza delle interazioni. Questi risultati confermano che la rete di USDT si struttura attorno a entità centralizzate che operano come punti di aggregazione per il flusso di valore, risultando in un grafo altamente disassortativo, dove i nodi più piccoli si collegano preferenzialmente ai grandi hub. L'analisi dell'harmonic centrality ha evidenziato la presenza di nodi come MetaMask o Gate.io, che fungono da gateway locali, migliorando l'accessibilità all'interno di cluster specifici. Questi nodi sono importanti per mantenere la resilienza della rete in caso di malfunzionamento degli hub globali. Inoltre [74] afferma che Bitfinex è indicato come un attore chiave nelle ondate speculative con effetti a catena su Bitcoin e altri asset. Questo pattern sembra essere coerente con il fenomeno "*rich-get-richer*", dove pochi nodi accumulano la maggior parte delle connessioni e del valore transazionale. Osserviamo tuttavia che la verifica della sussistenza di tale fenomeno richiederebbe analisi più approfondite che risultano al di fuori dello scopo di questa tesi.



(a) (b) (c) (d)

Figura 6.31: Grafici a barre per i top 10 nodi per centralità del token USDC.

N°	Nome
29	Circle
67	HitBTC 3
25	Nexo 2
13	0x56...bf9
8	Crypto.com 2
54	Crypto.com
53	FTX
65	Compound: cUSDC Token
62	HitBTC 2
60	Binance

(a)

N°	Nome
25	Nexo 2
60	Binance
23	Binance 2
51	Binance 3
20	Binance 4
16	Kraken 10
8	Crypto.com 2
53	FTX
29	Circle
48	UniSwap V2: USDC

(b)

N°	Nome
13	0x56...bf9
29	Circle
48	UniSwap V2: USDC
26	UniSwap V2: USDC-USDT
22	MEV Bot: 0xa57...6CF
55	UniSwap: USDC
1	SushiSwap: USDC
52	MEV Bot: 0x000...f56
24	0x: Exchange Proxy Fl. Wal.
31	MetaMask: Swaps Spender

(c)

N°	Nome
13	0x56...bf9
48	UniSwap V2: USDC
3	Coinbase 36
1	SushiSwap: USDC
30	0xe7...00a
24	0x: Exchange Proxy Fl. Wal.
26	UniSwap V2: USDC-USDT
22	MEV Bot: 0xa57...6CF
52	MEV Bot: 0x000...f56
31	MetaMask: Swaps Spender

(d)

Figura 6.32: Tabelle mapping (N°,Nome) del Grafico 6.31 - USDC.

L'analisi delle centralità per USDC, presentata nelle Figure 6.31 e 6.32, riflette le caratteristiche di una rete strettamente legata alla natura fiat-collateralizzata del

token, ma con alcune differenze rispetto a USDT. La rete di USDC, pur condividendo con USDT una marcata centralizzazione attorno a pochi nodi globalmente rilevanti, mostra una maggiore fiducia nella trasparenza delle sue operazioni, come evidenziato dalla presenza di nodi istituzionali come Circle e Coinbase. Questi nodi agiscono come garanti del sistema, gestendo flussi significativi di USDC e rafforzando la percezione di stabilità della rete. Circle in particolare è il nodo centrale che emette USDC, garantendo trasparenza dei flussi di token tra utenti ed exchange. Dallo studio degli hub score e centralità armoniche emergono nodi come UniSwap e SushiSwap, che contribuiscono liquidità attraverso protocolli decentralizzati. Tali nodi svolgono un ruolo cruciale nel connettere sotto-grafi regionali o specifici a una rete più ampia, migliorando la connettività interna. Tuttavia questi cluster locali sono collegati tra di loro ottenendo un'alta connettività nella rete.

Infine, nelle Figure 6.33 e 6.34, sono riportati i risultati dell'analisi delle centralità per WETH. A differenza delle stablecoin, la rete presenta caratteristiche strutturali uniche che possono essere direttamente correlate alla sua centralità nelle applicazioni DeFi. L'analisi dei nodi principali, combinata con i risultati della sezione topologica 6.2, consente di comprendere come le proprietà della rete WETH emergano da queste interazioni dense e altamente focalizzate. Per questo token, i nodi che appaiono frequentemente nelle top 100 globali e temporali includono indirizzi cruciali legati ai protocolli DeFi, come pool di liquidità di Uniswap, contratti di Router 2 e specifici MEV Bot.

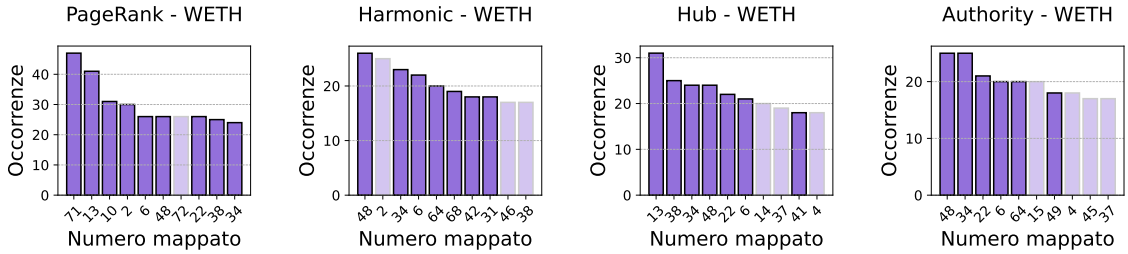
- **Pool di liquidità**. Un esempio di questa tipologia di nodi è rappresentato da UniSwap. Questi nodi hanno un elevato PageRank e Authority score, indicando il loro ruolo come punti di ricezione di grandi volumi di transazioni. Come confermato nella Sezione 6.2.3, questi pool contribuiscono a un'elevata forza (strength) in ingresso e in uscita, in quanto centralizzano grandi volumi transazionali. L'elevato Authority score è probabilmente dato dal fatto che spesso utenti che hanno molti ETH interagiscono con UniSwap per depositare collaterale, o meglio con smart contract per convertirli in WETH.

- **MEV Bot**. La presenza di questi nodi riflette strategie di arbitraggio e ottimizzazione, particolarmente rilevanti nei contesti di alta intensità transazionale. Questo è coerente con la reciprocità elevata osservata per WETH nella Sezione 6.2.2, dove le transazioni cicliche dominano la rete.

- **Contratti Router 2**: Come `UniSwapV2Router02`, svolgono un ruolo fondamentale nella gestione di operazioni complesse in piattaforme di scambio decentralizzate (DEX), facilitando l'esecuzione di transazioni, scambi multi-hop e l'aggiunta o rimozione di liquidità in modo ottimizzato [75].

Nella rete di WETH, nodi con molte connessioni non necessariamente gestiscono grandi volumi transazionali: i nodi centrali sono "facilitatori" di liquidità piuttosto

che accumulatori di valore diretto, coerentemente con quanto visto sulle correlazioni tra gradi e forze per WETH (Figura 6.17d).



(a) (b) (c) (d)

Figura 6.33: Grafici a barre per i top 10 nodi per centralità del token WETH.

N°	Nome
71	OpenSea: Wallet
13	0x56...bf9
10	Sky: MCD Join ETH A
2	Sky: Contract 1
6	UniSwap V2: DAI
48	UniSwap V2: USDC
72	0x69...b5d
22	MEV Bot: 0xa57...6CF
38	UniSwap V2: Router 2
34	UniSwap V2: USDT

(a)

N°	Nome
48	UniSwap V2: USDC
2	Sky: Contract 1
34	UniSwap V2: USDT
6	UniSwap V2: DAI
64	UniSwap V2: HEX
68	UniSwap V2: WBTC
42	UniSwap V2: LINK
31	MetaMask: Swaps Spender
46	0x85...38b
38	UniSwap V2: Router 2

(b)

N°	Nome
13	0x56...bf9
38	UniSwap V2: Router 2
34	UniSwap V2: USDT
48	UniSwap V2: USDC
22	MEV Bot: 0xa57...6CF
6	UniSwap V2: DAI
14	0xf7...82a
37	0xd9...830
41	0x: Exchange
4	asteriscus.eth

(c)

N°	Nome
48	UniSwap V2: USDC
34	UniSwap V2: USDT
22	MEV Bot: 0xa57...6CF
6	UniSwap V2: DAI
64	UniSwap V2: HEX
15	0xc3...327
49	0xfa...def
4	asteriscus.eth
45	0xa4...4c2
37	0xd9...830

(d)

Figura 6.34: Tabelle mapping (N°,Nome) del Grafico 6.33 - WETH.

Il ruolo centrale di UniSwap

I risultati mostrano che *UniSwap* occupa una posizione trasversale e centrale in tute le reti analizzate e nella maggior parte delle metriche di centralità. Questo riflette il suo ruolo cruciale nell'ecosistema DeFi come primo exchange decentralizzato basato su pool di liquidità, che garantisce scambi rapidi e accesso decentralizzato a una vasta gamma di token ERC-20 [76]. Per DAI, ad esempio, UniSwap gestisce importanti volumi di transazioni, fungendo sia da punto di scambio che da piattaforma per la gestione delle riserve. Analogamente, in USDT e USDC facilita la stabilità e l'efficienza delle transazioni, mentre per WETH consolida la sua importanza grazie all'integrazione dei principali protocolli DeFi.

Capitolo 7

Discussione dei risultati

In questa tesi abbiamo concentrato la nostra attenzione su quattro token ERC-20 fondamentali nell'ecosistema Ethereum: Tether USD (USDT), USD Coin (USDC), DAI Stablecoin (DAI) e Wrapped Ether (WETH). La scelta di questi token non è stata casuale, bensì una strategia per rappresentare diverse categorie di stablecoin e il ruolo distintivo di un token "wrapped" come WETH. La letteratura esistente ha già evidenziato l'importanza di questi asset, ma spesso si è limitata a un'analisi generica o statica delle loro reti transazionali. Il nostro studio, invece, si distingue per l'approccio sistematico e dinamico, combinando analisi globali e temporali per cogliere le sfumature evolutive di ciascun token.

Un aspetto distintivo del nostro lavoro è la metodologia adottata. Abbiamo costruito grafi globali e temporali per ciascun token, includendo informazioni fondamentali come il numero di transazioni e la quantità di token trasferiti. Questo approccio ci ha permesso di osservare non solo le proprietà statiche delle reti, ma anche la loro evoluzione nel tempo, evidenziando variazioni strutturali e dinamiche di utilizzo. Rispetto a [77] e [31], che analizzano molteplici reti ERC-20, il nostro lavoro si focalizza sulla peculiarità specifiche dei quattro token selezionati, fornendo una comprensione più profonda del loro ruolo nell'ecosistema.

Particolarmente interessante è il comportamento di WETH, che si differenzia dalle stablecoin per essere una rete più frammentata ma con una maggiore densità e reciprocità. I nostri risultati mostrano che, mentre USDT e USDC hanno una forte centralizzazione attorno a nodi come Binance e Bitfinex, caratteristica già osservata in [74], WETH presenta invece un'organizzazione topologica diversa, con cluster locali strettamente connessi. Questi cluster derivano non solo dall'uso intensivo di WETH nei pool di liquidità, come UniSwap, ma anche dall'attività ciclica tipica dei protocolli di lending e borrowing, dove viene frequentemente utilizzato come collaterale. Un elemento chiave che emerge dal nostro studio è il ruolo di WETH come asset principale nei *market maker automatizzati (AMM)*, come *UniSwap*. Questi sistemi si basano su algoritmi per determinare il prezzo degli asset in tempo reale e

richiedono asset altamente liquidi per garantire la stabilità delle operazioni. WETH, grazie alla sua natura fungibile e alla compatibilità con lo standard ERC-20, si presta particolarmente bene a questo scopo, fungendo da ponte tra ETH nativo e altri token ERC-20. La nostra analisi suggerisce che la centralità di WETH nella rete sia dovuta al suo utilizzo diffuso nei pool di liquidità, che rappresentano nodi cruciali per il funzionamento degli AMM. Questo risultato è coerente con quanto riportato in [78], che evidenzia come asset ad alta liquidità, come WETH, siano fondamentali per ridurre la volatilità e garantire la funzionalità dei pool. Sebbene non sia oggetto primario del nostro studio entrare nei dettagli del funzionamento economico di questi sistemi, il comportamento osservato della rete di WETH conferma la sua importanza strutturale all'interno dell'ecosistema Ethereum. La frammentazione osservata nella rete di WETH, con una copertura SCC più bassa rispetto alle stablecoin, potrebbe riflettere una struttura altamente specializzata e ciclica. È ipotizzabile che piccoli cluster di nodi interagiscano ripetutamente per supportare protocolli DeFi, creando sottoreti locali con maggiore densità e reciprocità rispetto a quelle osservate nelle reti di stablecoin. Queste caratteristiche potrebbero essere legate al ruolo ipotizzato di WETH come collaterale chiave per operazioni finanziarie decentralizzate, che favorirebbe la formazione di cluster locali più connessi. Tuttavia, come suggerito in [30], WETH è vincolato principalmente all'interno dell'ecosistema Ethereum, il che potrebbe limitarne l'interoperabilità al di fuori di questa rete. Questo aspetto potrebbe spiegare la piccola cerchia di utenti e la frammentazione osservata nella rete di WETH rispetto a quella delle stablecoin, che tendono invece a mostrare una maggiore espansione globale grazie alla loro natura intrinsecamente interoperabile e alla centralizzazione attorno a grandi exchange.

I test statistici condotti rivelano che nessuna delle reti analizzate segue rigorosamente una distribuzione power law. Sebbene le distribuzioni dei gradi presentino un'apparente somiglianza con il modello, il p-value inferiore a 0.1 nei test di conformità evidenzia deviazioni significative. Questo risultato si allinea con quanto riportato da [31], dove l'analisi su 100 reti di token ERC-20 ha confermato che la maggior parte presenta un p-value nullo. La nostra analisi ha evidenziato che le reti studiate mostrano caratteristiche pseudo-hub-centriche, ovvero una forte concentrazione di connessioni in pochi nodi ad alto grado. Questo pattern è coerente con quanto riportato in [77], che identifica una gerarchia basata su hub centrali, come grandi exchange o smart contract.

Abbiamo inoltre osservato che, sebbene le reti ERC-20 siano efficienti nella propagazione dell'informazione in quanto il diametro è nell'ordine del logaritmo dei nodi, questa efficienza globale non si traduce in una coesione locale. I coefficienti di clustering globali delle reti risultano bassi, indicando connessioni locali deboli e una scarsità di triangoli. Questo risultato è coerente quanto riportato in [66], dove si evidenzia che le reti ERC-20 mostrano un clustering significativamente inferiore

ad altre reti transazionali, e in [31], che attribuisce l'assenza di clustering locale a una forte centralizzazione e a strutture disassortative. Le stablecoin, in particolare, mostrano una topologia hub-and-spoke, dominata da pochi nodi centrali altamente connessi che attraggono la maggior parte del flusso transazionale. Questo fenomeno riduce la coesione locale, lasciando i wallet periferici isolati tra loro, ma garantisce comunque un'efficienza globale grazie alla presenza di questi hub centrali. Questo risultato trova conferma in [74], che descrive che la rete di USDT come una struttura fortemente centralizzata e fragile, e in [79], che sottolinea la concentrazione delle risorse in pochi nodi chiave. Infine, la nostra analisi conferma che le reti ERC-20 analizzate si collocano al confine tra efficienza globale e frammentazione locale, senza rientrare nella categoria di reti small-world. Sebbene il diametro basso indichi una propagazione dell'informazione rapida, l'insufficienza del clustering e la frammentazione strutturale impediscono a queste reti di sviluppare proprietà small-world, come confermato anche in [66] e [31].

Tutte le reti analizzate confermano un comportamento disassortativo, sia per i gradi che per le forze. Questo implica che i nodi con molte connessioni (o alto volume transazionale) tendono a collegarsi a nodi meno connessi o con volumi inferiori, anziché formare cluster di nodi altamente connessi tra loro. Tale risultato si allinea con quanto riportato in [31] che ha evidenziato una disassortatività generalizzata nelle reti ERC-20. Tuttavia, il nostro studio si distingue perché introduce l'analisi della disassortatività delle forze, mostrando come la struttura disassortativa non riguardi solo il numero di connessioni, ma anche i volumi delle transazioni. Tra i token analizzati, WETH risulta meno disassortativo rispetto agli altri, pur mantenendo un comportamento complessivamente disassortativo. Questo potrebbe essere attribuito alla sua funzione principale nei protocolli DeFi, dove i volumi transazionali sono distribuiti in modo relativamente uniforme tra i cluster locali creati per le operazioni di lending, borrowing e pool di liquidità. In contrasto, USDT e USDC presentano una disassortatività più marcata, coerente con una rete polarizzata attorno a grandi exchange come Binance e Bitfinex, che fungono da hub principali per la maggior parte delle transazioni. DAI, invece, si colloca in una posizione intermedia: la sua disassortatività, pur essendo evidente, è meno estrema rispetto alle stablecoin fiat-collateralizzate, probabilmente per la natura decentralizzata e il ruolo distribuito dei nodi nella gestione del token. Inoltre tutte le reti mostrano una correlazione alta tra i gradi in ingresso e in uscita, il che indica un bilanciamento tra il numero di connessioni ricevute ed inviate dai nodi. Questo è particolarmente evidente per DAI e WETH, dove i nodi tendono a mantenere un equilibrio tra connessioni entranti e uscenti. La correlazione più debole osservata per USDT suggerisce una maggiore polarizzazione della rete, con alcuni nodi che concentrano un numero elevato di connessioni in ingresso o in uscita. Per quanto riguarda le forze, si nota una correlazione più debole. Questo risultato evidenzia che il volume delle transazioni non

è necessariamente proporzionale al numero di connessioni: nodi con molte, come grandi hub centralizzati di USDT e USDC, gestiscono enormi volumi transazionali, accentuando il divario con i nodi periferici meno connessi. Al contrario, in DAI e WETH, le forze sono distribuite in modo più equilibrato, riflettendo in misura maggiore il numero di connessioni. Questo implica che i volumi transazionali nei grafi di WETH e DAI tendono ad essere più proporzionali alla struttura delle connessioni, riducendo la centralizzazione attorno a pochi nodi dominanti.

A differenza delle stablecoin fiat, DAI si basa su un meccanismo di sovra-collateralizzazione decentralizzato, il quale potrebbe spiegare alcune dinamiche simili a quelle osservate in WETH. Ad esempio, il fatto che gli utenti debbano depositare asset come ETH per generare DAI potrebbe contribuire a creare una struttura di rete in cui i nodi centrali svolgono un ruolo cruciale. Questa sovra-collateralizzazione, unita a l'utilizzo di DAI nei protocolli di lending e borrowing, potrebbe essere alla base della maggiore reciprocità osservata rispetto alle stablecoin fiat. I cicli di prestiti e restituzioni che caratterizzano i protocolli DeFi potrebbero infatti alimentare interazioni ripetute tra nodi, generando una rete con un comportamento parzialmente ciclico. Tuttavia, la frammentazione della rete di DAI appare più bassa rispetto a quella di WETH. Questo potrebbe essere dovuto al fatto che DAI, a differenza di WETH, non è limitato a un uso strettamente legato ai pool di liquidità ma viene utilizzato in una varietà più ampia di contesti, inclusi protocolli di pagamento e riserva di valore. Sebbene entrambe le reti mostrino una concentrazione attorno a pochi nodi centrali, come osservato nei nostri risultati sperimentali, DAI tende a mostrare una distribuzione più uniforme delle connessioni rispetto a WETH, il che potrebbe riflettere una rete meno specializzata.

L'analisi della centralità ci ha permesso di individuare nodi altamente centrali in ogni rete dei token analizzati. [74] ha evidenziato che, nella rete USDT nodi centrali come HTX (Houbi), Bifinex e Binance predominano la rete in termini di connessioni. Evidenzia il potenziale ruolo di Tether nel creare instabilità nei mercati delle criptovalute dove Bifinex è indicato come un attore chiave nelle ondate speculative con effetti a catena su Bitcoin e altri asset. Questo pattern è coerente con il fenomeno "*rich-gets-richer*", dove pochi nodi accumulano la maggior parte delle connessioni e del valore transazionale. La struttura disassortativa, con connessioni tra nodi di alto e basso grado, aumenta tale fragilità. Infatti la rete non presenta proprietà small-world, riflettendo una topologia dispersiva con interazioni prevalentemente unidirezionali e una debole reciprocità. Contrariamente, la rete di WETH, si distingue per una decentralizzazione maggiore, con nodi centrali rappresentati principalmente da pool di liquidità come UniSwap, e smart contract per la conversione del token stesso. L'harmonic centrality elevata riflette una connettività più forte tra le reti, conforme anche per un diametro ridotto delle reti stesse.

Capitolo 8

Conclusione

Questo lavoro ha permesso di comprendere in profondità le dinamiche e le caratteristiche delle reti transazionali dei principali token ERC-20, fornendo una visione sistematica e dinamica dell'ecosistema Ethereum. Attraverso l'analisi di metriche topologiche e strutturali, sia a livello globale che temporale, abbiamo fornito strumenti per interpretare il ruolo e il comportamento di diversi tipi di token, evidenziando come la loro funzione economica influenzi la rete di interazioni.

Analizzare diversi tipi di token, soprattutto le stablecoin, ci ha permesso di studiare il comportamento della rete, come gli attori principali influiscono su di essa e cosa cambia nel tempo. Inoltre il confronto tra due tipi diversi di stableocoin ci ha permesso di comprendere a pieno la differenza tra stablecoin con diverso tipo di collateralizzazione. Analizzare invece un token wrappato è stato utile per comprendere come viene integrato nel sistema ERC-20, come ha avuto un impatto nell'utilizzo del token in protocolli decentralizzati, rendendo possibile l'utilizzo della criptovaluta nativa di Ethereum.

Le implicazioni di questo studio vanno oltre la semplice descrizione delle reti. Abbiamo sviluppato un approccio che può essere applicato per monitorare l'evoluzione delle reti blockchain sia per rilevare pattern utili alla progettazione che per ottimizzare di nuovi protocolli DeFi o di gestione delle stablecoin. La metodologia adottata, con la sua attenzione ai dettagli strutturali e dinamici, offre una base solida per ulteriori studi sull'efficienza, la sicurezza e la sostenibilità delle reti basate su blockchain.

Infine, il confronto con la letteratura esistente ha permesso di collocare i risultati ottenuti all'interno di un quadro più ampio, contribuendo a chiarire la natura complessa e multi-dimensionale delle reti ERC-20. Questo lavoro, quindi, non solo arricchisce la comprensione teorica delle reti transazionali, ma fornisce spunti pratici per migliorare le infrastrutture esistenti e supportare l'adozione di soluzioni decentralizzate.

8.1 Sviluppi futuri

Le analisi svolte in questa tesi aprono molteplici possibilità per ampliare la ricerca e approfondire la comprensione delle reti transazionali ERC-20. In particolare, i seguenti sviluppi futuri potrebbero rappresentare un significativo contributo sia dal punto di vista teorico che applicativo:

- **Estensione a nuovi token**: L'estensione delle analisi a un numero maggiore di token ERC-20 potrebbe aiutare a comprendere meglio le differenze strutturali e funzionali tra le reti. Includere token con scopi differenti, come *governance token* e token legati a specifici protocolli DeFi, permetterebbe di analizzare una gamma più ampia di dinamiche economiche e sociali.

- **Analisi delle stablecoin algoritmiche**: Le stablecoin algoritmiche rappresentano un'interessante evoluzione nel panorama delle criptovalute, grazie ai loro meccanismi di stabilizzazione innovativi basati su algoritmi. Estendere l'analisi a queste stablecoin potrebbe evidenziare pattern di comportamento unici e fornire una migliore comprensione del loro funzionamento all'interno dell'ecosistema DeFi. Ad esempio, si potrebbero confrontare le loro reti con quelle delle stablecoin collateralizzate fiat e cripto, analizzando differenze in termini di decentralizzazione, resilienza agli shock e volatilità.

- **Community Detection**: L'applicazione di algoritmi di rilevamento delle comunità come Louvain, consentirebbe di identificare cluster di nodi che interagiscono più frequentemente tra loro. Questo approccio potrebbe essere utilizzato per identificare gruppi di utenti con comportamenti simili e rivelare la formazione di comunità in protocolli DeFi. Inoltre, l'analisi delle comunità temporali potrebbe chiarire come le reti si trasformano nel tempo, evidenziando la nascita o la dissoluzione di comunità in seguito a eventi rilevanti.

- **Analisi evento-centrica**: Una direzione promettente potrebbe essere l'applicazione di analisi focalizzate su eventi specifici, come il crollo di TerraUSD o l'introduzione di nuove regolamentazioni. Questi studi potrebbero aiutare a chiarire come le reti reagiscono a eventi estremi, mostrando adattamenti nelle topologie delle reti o cambiamenti nei nodi più influenti.

- **Microvelocity**: Un aspetto innovativo è l'adattamento del concetto di Microvelocity al modello account-based di Ethereum, superando i limiti intrinseci di questa architettura rispetto al modello UTXO. La Microvelocity permette di calcolare con precisione la velocità con cui un valore viene speso, tracciando ogni unità monetaria lungo il suo ciclo di vita. Tuttavia, nel contesto ERC-20, caratterizzato da bilanci aggregati, non è possibile distinguere con

certezza quale porzione del valore in un account venga spesa in un determinato momento [80]. La principale sfida nel calcolo della Microvelocity nei token ERC-20 risiede nell'impossibilità di associare direttamente un'unità economica al suo tempo di holding a livello individuale. Per affrontare questa difficoltà, si potrebbe adottare un approccio basato su:

- Analizzare la cronologia delle transazioni entranti e uscenti di ogni nodo, associando il tempo di holding al valore economico tra una transazione in entrata e la successiva in uscita.
- Calcolare la distribuzione del tempo di detenzione dei valori in base alle transazioni aggregate, normalizzandola sul totale delle transazioni per nodo.
- Introdurre una ponderazione basata sul valore delle transazioni, in modo da differenziare il contributo delle transazioni di grande valore rispetto a quelle minori.

Questo calcolo della Microvelocity per ogni nodo permetterebbe di identificare nodi con alta o bassa velocità di circolazione economica, distinguendo tra wallet personali, grandi exchange e protocolli DeFi. Inoltre valutare se la ricchezza circola rapidamente in specifiche sottoreti o rimane intrappolata in nodi centralizzati potrebbe dimostrare il comportamento delle reti in specifici periodi di attività. Ad esempio, ci aspettiamo che nel periodo del crollo di TerraUSD ci sia un aumento della velocità dei nodi nel trasferimento di token verso lo smart contract della stablecoin, per riottenere il capitale depositato (in fiat o criptovalute). Infine è utile anche osservare l'andamento temporale della Microvelocity, correlando i risultati topologici e strutturali della rete.

Bibliografia

[1] Gavin Wood et al. «Ethereum: A secure decentralised generalised transaction ledger». In: *Ethereum project yellow paper* 151.2014 (2014), pp. 1–32.

[2] Gabor Csardi e Tamas Nepusz. «The igraph software». In: *Complex syst* 1695 (2006), pp. 1–9.

[3] Paolo Boldi e Sebastiano Vigna. «The webgraph framework I: compression techniques». In: *Proceedings of the 13th international conference on World Wide Web*. 2004, pp. 595–602.

[4] Satoshi Nakamoto. «Bitcoin: A peer-to-peer electronic cash system». In: *Satoshi Nakamoto* (2008).

[5] Ralph C. Merkle. «Protocols for Public Key Cryptosystems». In: *Proceedings of the 1980 IEEE Symposium on Security and Privacy*. Oakland, California, USA, 14-16 April 1980: IEEE Computer Society, 1980, pp. 122–134. DOI: 10.1109/SP.1980.10006. URL: https://doi.org/10.1109/SP.1980.10006.

[6] Sunny King e Scott Nadal. «Ppcoin: Peer-to-peer crypto-currency with proof-of-stake». In: *self-published paper, August* 19.1 (2012).

[7] Vitalik Buterin et al. «A next-generation smart contract and decentralized application platform». In: *white paper* 3.37 (2014), pp. 2–1.

[8] M Poongodi et al. «Prediction of the price of Ethereum blockchain cryptocurrency in an industrial finance system». In: *Computers & Electrical Engineering* 81 (2020), p. 106527.

[9] Ethereum Foundation. *Ethereum transactions*. https://ethereum.org/en/developers/docs/transactions/. Accessed: 2024-10-12. 2024.

[10] Ethereum Foundation. *Gas EVM Transactions*. https://ethereum.org/en/developers/docs/evm/. Accessed: 2024-10-12. 2024.

[11] Don Johnson, Alfred Menezes e Scott Vanstone. «The elliptic curve digital signature algorithm (ECDSA)». In: *International journal of information security* 1 (2001), pp. 36–63.

[12] Donald R. Morrison. «PATRICIA - Practical Algorithm To Retrieve Information Coded in Alphanumeric». In: *J. ACM* 15.4 (1968), pp. 514–534. DOI: 10.1145/321479.321481. URL: https://doi.org/10.1145/321479.321481.

[13] Andreas M Antonopoulos e Gavin Wood. *Mastering ethereum: building smart contracts and dapps*. O'reilly Media, 2018.

[14] Maximilian Wohrer e Uwe Zdun. «Smart contracts: security patterns in the ethereum ecosystem and solidity». In: *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*. IEEE. 2018, pp. 2–8.

[15] Tharaka Hewa, Mika Ylianttila e Madhusanka Liyanage. «Survey on blockchain based smart contracts: Applications, opportunities and challenges». In: *Journal of network and computer applications* 177 (2021), p. 102857.

[16] Nicola Atzei, Massimo Bartoletti e Tiziana Cimoli. «A survey of attacks on ethereum smart contracts (sok)». In: *Principles of Security and Trust: 6th International Conference, POST 2017, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2017, Uppsala, Sweden, April 22-29, 2017, Proceedings 6*. Springer. 2017, pp. 164–186.

[17] Zibin Zheng et al. «An overview on smart contracts: Challenges, advances and platforms». In: *Future Generation Computer Systems* 105 (2020), pp. 475–491.

[18] Maher Alharby e Aad Van Moorsel. «Blockchain-based smart contracts: A systematic mapping study». In: *arXiv preprint arXiv:1710.06372* (2017).

[19] Fabian Vogelsteller e Vitalik Buterin. «ERC-20 token standard». In: *Ethereum Foundation (Stiftung Ethereum), Zug, Switzerland* 169 (2015).

[20] Harry Kalodner et al. «Arbitrum: Scalable, private smart contracts». In: *27th USENIX Security Symposium (USENIX Security 18)*. 2018, pp. 1353–1370.

[21] christianb93. *Basis structure of a token and the ERC20 standard*. https://leftasexercise.com/2021/08/29/basis-structure-of-a-token-and-the-erc20-standard/. 2021.

[22] ig.com. *Moneta fiat (definizione)*. https://www.ig.com/it/glossario-trading/definizione-di-moneta-fiat.

[23] Erik Anderson. *An Introduction to Stablecoins*. https://www.globalxetfs.com/an-introduction-to-stablecoins/. 2023.

[24] Martin Brennecke et al. «The de-central bank in decentralized finance: A case study of MakerDAO». In: (2022).

[25] Maker Foundation. «The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System». In: (2020).

[26] Vladimir Nurbaev, Cheuk Hang Au e Chih-Yuan Chou. «When Stablecoin is No Longer Stable-A Case Study on the Failure of TerraUSD». In: (2023).

[27] Alex Williams. *Sushiswap Vs. Uniswap: What Are the Differences?* `https://builtin.com/blockchain/sushiswap-vs-uniswap`. 2022.

[28] Sam Werner et al. «Sok: Decentralized finance (defi)». In: *Proceedings of the 4th ACM Conference on Advances in Financial Technologies*. 2022, pp. 30–46.

[29] Michelle Lodge. *Yield Farming: The Truth About This Crypto Investment Strategy*. `https://www.investopedia.com/what-is-yield-farming-7098519`. 2024.

[30] Giulio Caldarelli. «Wrapping trust for interoperability: A preliminary study of wrapped tokens». In: *Information* 13.1 (2021), p. 6.

[31] Matteo Loporchio et al. «Analysis and Characterization of ERC-20 Token Network Topologies». In: *International Conference on Complex Networks and Their Applications*. Springer. 2023, pp. 344–355.

[32] Tether Operations Limited. *Tether*. `https://assets.ctfassets.net/vyse88cgwfbl/5UWgHMvz071t2Cq5yTw5vi/c9798ea8db99311bf90ebe0810938b01/TetherWhitePaper.pdf`. 2013.

[33] coinDesk. *As Tether Supply Hits Record Highs, It Moves Away From Original Home*. `https://www.coindesk.com/tech/2020/05/05/as-tether-supply-hits-record-highs-it-moves-away-from-original-home/`.

[34] Wen Shou Hsu e Cheuk Hang Au. «Revealing stablecoin successes: Lessons from a case study on USDT». In: (2023).

[35] Coinbase. *Ushering in the next chapter for USDC*. `https://www.coinbase.com/it/blog/ushering-in-the-next-chapter-for-usdc`. 2023.

[36] Binance Academy. *BEP-20*. `https://academy.binance.com/en/glossary/bep-20`.

[37] Binance Academy. *SPL*. `https://academy.binance.com/en/glossary/spl`.

[38] USA. *An official website of the United States Government*. `https://www.fincen.gov/`.

[39] Circle. *Transparency & Stability*. `https://www.circle.com/en/transparency`.

[40] MakerDAO. *The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System*. `https://makerdao.com/en/whitepaper/`.

[41] Wikipedia. *Terra Blockchain*. `https://en.wikipedia.org/wiki/Terra_(blockchain)`.

[42] Jiageng Liu, Igor Makarov e Antoinette Schoar. *Anatomy of a run: The terra luna crash*. Rapp. tecn. National Bureau of Economic Research, 2023.

[43] Arijit Khan. «Graph analysis of the ethereum blockchain data: A survey of datasets, methods, and future work». In: *2022 IEEE International Conference on Blockchain (Blockchain)*. IEEE. 2022, pp. 250–257.

[44] Fan Chung. «A Brief Survey of PageRank Algorithms.» In: *IEEE Trans. Netw. Sci. Eng.* 1.1 (2014), pp. 38–42.

[45] Albert-László Barabási e Réka Albert. «Emergence of scaling in random networks». In: *science* 286.5439 (1999), pp. 509–512.

[46] Klaudia Jarno e Hanna Kolodziejczyk. «Does the design of stablecoins impact their volatility?» In: *Journal of Risk and Financial Management* 14.2 (2021), p. 42.

[47] Andres Garcia-Medina e Jose B Hernandez C. «Network analysis of multivariate transfer entropy of cryptocurrencies in times of turbulence». In: *Entropy* 22.7 (2020), p. 760.

[48] Orsolya Kardos, Andras London e Tamas Vinko. «Stability of network centrality measures: a numerical study». In: *Social Network Analysis and Mining* 10 (2020), pp. 1–17.

[49] Gabor Csardi e Tamas Nepusz. «The igraph software». In: *Complex syst* 1695 (2006), pp. 1–9.

[50] The igraph core team. *Igraph C documentation*. `https://igraph.org/c/doc/`.

[51] The igraph core team. *Igraph C documentation: Chapter 21. Reading and writing graphs from and to files*. `https://igraph.org/c/doc/igraph-Foreign.html`.

[52] The igraph core team. *Igraph C documentation: Chapter 13. Structural properties of graphs*. `https://igraph.org/c/doc/igraph-Structural.html`.

[53] Paolo Boldi e Sebastiano Vigna. «In-core computation of geometric centralities with hyperball: A hundred billion nodes and beyond». In: *2013 IEEE 13th International Conference on Data Mining Workshops*. IEEE. 2013, pp. 621–628.

[54] Stefan Heule, Marc Nunkesser e Alexander Hall. «Hyperloglog in practice: Algorithmic engineering of a state of the art cardinality estimation algorithm». In: *Proceedings of the 16th International Conference on Extending Database Technology*. 2013, pp. 683–692.

[55] Aaron Clauset, Cosma Rohilla Shalizi e Mark EJ Newman. «Power-law distributions in empirical data». In: *SIAM review* 51.4 (2009), pp. 661–703.

[56] Frank J. Massey. «The Kolmogorov-Smirnov Test for Goodness of Fit». In: *Journal of the American Statistical Association* 46.253 (1951), pp. 68–78. ISSN: 01621459, 1537274X. URL: http://www.jstor.org/stable/2280095 (visitato il giorno 28/10/2024).

[57] Deepak Ajwani, Ulrich Meyer e Vitaly Osipov. «Breadth First Search on Massive Graphs.» In: *The Shortest Path Problem*. 2006, pp. 291–307.

[58] Duncan J Watts e Steven H Strogatz. «Collective dynamics of 'small-world'networks». In: *nature* 393.6684 (1998), pp. 440–442.

[59] Rogier Noldus e Piet Van Mieghem. «Assortativity in complex networks». In: *Journal of Complex Networks* 3.4 (2015), pp. 507–542.

[60] Lawrence Page et al. *The PageRank Citation Ranking: Bringing Order to the Web.* Technical Report 1999-66. Previous number = SIDL-WP-1999-0120. Stanford InfoLab, nov. 1999. URL: http://ilpubs.stanford.edu:8090/422/.

[61] Scott Imig. «Trustworthiness and Pagerank on the Ethereum Blockchain: Technical Report». In: *Available at SSRN* (2023).

[62] David Gleich. *PRPACK*. https://github.com/dgleich/prpack.

[63] Yannick Rochat. «Closeness centrality extended to unconnected graphs: The harmonic centrality index». In: *Asna*. 2009.

[64] Jon M Kleinberg et al. «The web as a graph: Measurements, models, and methods». In: *Computing and Combinatorics: 5th Annual International Conference, COCOON'99 Tokyo, Japan, July 26–28, 1999 Proceedings 5*. Springer. 1999, pp. 1–17.

[65] Patrick Doreian e Andrej Mrvar. «Hubs and authorities in the Koch brothers network». In: *Social Networks* 64 (2021), pp. 148–157.

[66] Friedhelm Victor e Bianca Katharina Luders. «Measuring ethereum-based erc20 token networks». In: *Financial Cryptography and Data Security: 23rd International Conference, FC 2019, Frigate Bay, St. Kitts and Nevis, February 18–22, 2019, Revised Selected Papers 23*. Springer. 2019, pp. 113–129.

[67] Giulio Caldarelli. «Wrapping trust for interoperability: A preliminary study of wrapped tokens». In: *Information* 13.1 (2021), p. 6.

[68] Aave. *Aave Protocol Whitepaper*. https://github.com/aave/aave-protocol/blob/master/docs/Aave_Protocol_Whitepaper_v1_0.pdf.

[69] Zack Voell. *As Tether Supply Hits Record Highs, It Moves Away From Original Home*. https://www.coindesk.com/tech/2020/05/05/as-tether-supply-hits-record-highs-it-moves-away-from-original-home/.

[70] El Dorado. *Tether's Transparency Issues: Impact on Crypto Trading and Stability*. https://eldorado.io/pt/blog/tether-transparency-crypto-stability/.

[71] Stefano Boccaletti et al. «Complex networks: Structure and dynamics». In: *Physics reports* 424.4-5 (2006), pp. 175–308.

[72] Cos'è la criptovaluta Uniswap (UNI) e come funziona? *kriptomat*. https://kriptomat.io/it/quotazioni-criptovalute/uniswap-uni-valore/cosa-sono-i/.

[73] Cryptonomist. *Che cosa sono e come funzionano i MEV bot di Ethereum?* https://cryptonomist.ch/2023/05/28/cosa-sono-mev-bot-ethereum/.

[74] Giovanni Rosa e Remo Pareschi. «Tether: A Study on Bubble-Networks». In: *Frontiers in Blockchain* 4 (2021), p. 686484.

[75] UniSwap. *Router02*. https://docs.uniswap.org/contracts/v2/reference/smart-contracts/router-02.

[76] Uniswap: il primo exchange della DeFi. *academy*. https://academy.youngplatform.com/criptovalute/uniswap-cos-e-come-funziona/.

[77] Weili Chen et al. «Traveling the token world: A graph analysis of ethereum erc20 token ecosystem». In: *Proceedings of The Web Conference 2020*. 2020, pp. 1411–1421.

[78] Guillermo Angeris et al. «An analysis of Uniswap markets». In: (2021).

[79] Anton Wahrstätter. «Stablecoin billionaires-A descriptive analysis of the ethereum-based stablecoin ecosystem». In: *Available at SSRN 3737404* (2020).

[80] Carlo Campajola, Marco D'Errico e Claudio J Tessone. «MicroVelocity: rethinking the Velocity of Money for digital currencies». In: *arXiv preprint arXiv:2201.13416* (2022).