

Sviluppo di un token ERC-20 e di un exchange decentralizzato

Daniele Atzori, Paolo Bertin, Giovanni Roncoli

Università degli studi di Milano, Dipartimento di Fisica

24/07/2023

1 Abstract

In questa relazione descriviamo e commentiamo la realizzazione di un token ERC-20 e di un exchange decentralizzato con market making automatico. Il sistema è stato sviluppato tramite la creazione di smart contracts in linguaggio Solidity, lanciati sulla blockchain test di Sepolia. Questo exchange è stato utilizzato per una gara di trading tra i tre autori del progetto, della durata di cinque giorni: in questa relazione discutiamo anche le regole, l'andamento e il risultato di tale gara.

2 Introduzione ai sistemi di exchange decentralizzati

2.1 Come funziona un exchange decentralizzato

Un exchange decentralizzato (DEX) è una piattaforma che permette lo scambio di cryptovalute direttamente con altri utenti, senza l'intermediazione di un ente centrale. In particolare, in un DEX non vi è un ente che controlla i fondi depositati dagli utenti: non esiste il concetto di conto in cui gli utenti depositano le loro valute, ma possono attingere a queste direttamente dai loro wallet (protetti da una chiave privata in possesso del proprietario) per poterle scambiare.

Gli utenti possono scambiare crypto o, in generale, fare operazioni attraverso smart contracts, ovvero direttamente sulla blockchain (*on-chain*); esistono DEX che lavorano anche *off-chain*, ma non sono completamente decentralizzati. Attraverso gli smart contracts, un DEX collega acquirenti e venditori e calcola in automatico i tassi di scambio e le commissioni concernenti lo scambio di crypto, che tipicamente avvengono attraverso pool di liquidità, ossia "contenitori" di token che possono essere venduti e comprati.

2.2 Pro e contro dei DEX

I DEX presentano una serie di vantaggi e di svantaggi. I vantaggi principali sono i seguenti:

- i fondi non sono controllati da un ente centrale, dunque l'utente ne ha pieno possesso;
- non è necessaria la conferma dell'identità dell'utente;
- è possibile scambiare ogni tipo di crypto, anche quelle non tipicamente presenti negli exchange, a patto che siano compatibili con la blockchain.

Vi sono, però, anche una serie di svantaggi:

- tendenzialmente un exchange decentralizzato è poco user-friendly, dunque per i neofiti può essere più difficile da utilizzare;
- la liquidità non è garantita: è possibile scambiare crypto solo se esiste la controparte, e la presenza di quest'ultima non è garantita da un ente centrale;
- se l'utente perde la sua chiave privata, perde definitivamente l'accesso al suo wallet e quindi tutte le valute contenute;
- le commissioni nei DEX possono essere più alte rispetto ad exchange centralizzati.

2.3 Rischi principali

I maggiori rischi dei DEX sono legati alla mancata regolamentazione: infatti, chiunque può scaricare un wallet e iniziare a scambiare token, senza necessità di verifica della sua identità, e questo può permettere l'azione di operatori di token truffaldini. La natura aperta della blockchain, che rappresenta uno dei vantaggi dei DEX, può quindi comportare dei rischi, anche per via della mancanza di un quadro giuridico definito che permetterebbe alle istituzioni di agire per evitare possibili attacchi. Sempre legata alla natura aperta dei DEX, vi è la possibilità, per ogni utente, di sfruttare a proprio piacimento possibili bug o vulnerabilità negli smart contracts.

Un altro fattore di rischio piuttosto importante è costituito dal fatto che nelle blockchain le transazioni non sono istantanee e nei mercati delle crypto i prezzi possono cambiare nell'intervallo temporale in cui una transazione viene confermata; inoltre, lavorando *on-chain*, le transazioni sono soggette alla possibile congestione della rete, che aumenta i tempi di conferma e le commissioni.

3 Introduzione ai market making automatici

3.1 Cosa è un Market Maker Automatico?

I market maker automatizzati (AMM) sono un tipo exchange decentralizzato che riesce a definire un prezzo tra due quantità, basandosi su un algoritmo (a volte molto semplice, altre volte più complicato). Gli AMM possono fungere sia da venditori che da compratori, così da rimuovere la necessità di dover interagire necessariamente con un'altra persona fisica interessata all'exchange, permettendo una disponibilità di compravendita immediata.

Diversi sono le piattaforme di AMM oggi disponibili, le più note sono:

- Uniswap
- Curve
- Balancer

Alla base di un AMM ci sono le cosiddette "pool". Le pool possono essere definite come una collezione di crypto utilizzate per fare mercato e che qualsiasi persona fisica interessata ad esse può quindi comprare o vendere. Un concetto essenziale per la pool stessa è quello di "liquidità", ovvero la quantità di token presenti nella pool. Tale concetto risulta necessario per definire le variazioni di prezzo: in quanto, in una pool con una bassa liquidità, tali variazioni a seguito di operazioni di compravendita possono essere molto grandi, e viceversa. In questo modo, cioè basandosi sulla liquidità della pool stessa, è possibile ottenere una variazione di prezzo automatica, in base alla richiesta sul mercato dei token che la pool stessa mette a disposizione.

3.2 Diverse tipologie di AMM

Esistono diverse tipologie di AMM, le quali si differenziano principalmente per il metodo utilizzato per definire il prezzo del token nella pool.

3.2.1 AMM a funzione costante

I market maker a funzione costante, come ad esempio i market maker a prodotto costante o a somma costante, sono tipi di market maker, detti di prima generazione, resi popolari da protocolli come Uniswap, Curve o Bancor. Le pool sono definite attraverso degli smart contracts, e di conseguenza ciò che gli utenti fanno sono delle vere e proprie operazioni di exchange con uno smart contract.

3.2.2 Market maker a prodotto costante

Vediamo come esempio il market maker a prodotto costante. Questa tipologia si basa sulla funzione $x \cdot y = k$ dove x ed y rappresentano le quantità dei due token inseriti nella pool, mentre k è una costante.

La funzione appena citata quindi stabilisce il range di prezzo tra i due token a seconda della liquidità disponibile di ogni token. Questo significa che quando la riserva del primo token aumenta, allora diminuirà quella del secondo in maniera tale da mantenere, appunto, il prodotto costante. Ovviamente vale un ragionamento analogo per l'aumento del secondo token. Funzioni di questo tipo sono rappresentate da delle iperboli sul piano cartesiano.

3.2.3 Market maker a somma costante

Un altro esempio sono i market maker a somma costante. La formula qui utilizzata è invece $x + y = k$, la rappresentazione su un piano cartesiano è una retta che interseca entrambi gli assi: di conseguenza non è possibile avere una liquidità infinita, ma solo quella che permette alla x e alla y di essere compresi tra i valori zero e il punto di intersezione della retta, in quanto il piano cartesiano deve essere limitato al primo quadrante.

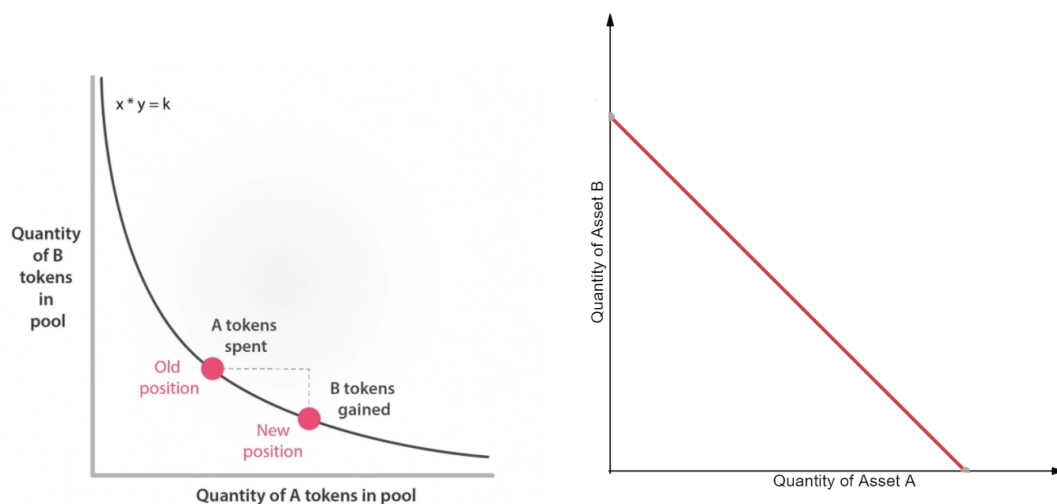


Figura 1: legge di un AMM a prodotto costante (a sinistra) e a somma costante (a destra).

4 Architettura del sistema implementato

L'exchange decentralizzato sviluppato per il progetto è diviso in 2 parti:

- gli smart contract scritti in linguaggio Solidity che vengono pubblicati nella rete blockchain, in cui tutti i nodi della rete possono interagire;
- i bot scritti in linguaggio python che simulano una clientela che compra e vende Token all'interno del mercato.

4.1 Smart contracts

Gli smart contracts sono i programmi alla base del funzionamento dell'exchange, contengono tre categorie principali di funzioni:

- il **costruttore**, nel quale vengono inseriti i dati iniziali del contratto e si attiva al momento della pubblicazione del medesimo;
- le **funzioni**, che possono essere eseguite mentre il contratto è pubblicato in rete, in base al loro tipo:
 - *private*, possono essere chiamate solo dal contratto stesso;
 - *internal*, possono essere chiamate dal contratto stesso e dai suoi ereditari;
 - *external*, possono essere chiamate solo da indirizzi esterni;
 - *public*, possono essere chiamate da chiunque all'interno della rete;
 - *view*, non modificano lo stato delle variabili;
- i **modificatori**, che contengono delle condizioni da verificare affinché una certa funzione possa essere chiamata; per esempio, il modificatore *OnlyOwner* richiede che l'indirizzo che sta chiamando la funzione del contratto sia quello dell'owner (ossia colui il quale ha lanciato il contratto sulla blockchain) e in caso negativo la funzione va in *revert* (l'operazione viene annullata e lo stato ritorna a quello iniziale prima della chiamata).

Sono presenti anche delle variabili di tipo **evento**, le quali accettano dei parametri che vengono indicizzati; queste variabili vengono poi chiamate tramite il comando *Emit* alla fine di una funzione e i parametri vengono salvati all'interno della blockchain; quest'operazione, per esempio, può essere utilizzata quando si vuole tenere traccia dei trasferimenti che avvengono all'interno della rete.

Insieme agli smart contracts vengono associati delle interfacce: queste sono contratti di tipo astratto, cioè contengono le funzioni del contratto principale, ma sono tutte di tipo *external* e sono vuote; le interfacce servono per poter chiamare funzioni di un contratto all'interno di un altro contratto.

4.1.1 Token - Paycoin

Nell'exchange realizzato, i Paycoin sono l'equivalente della moneta pubblica, mentre i Token sono la moneta di proprietà del loro creatore. Gli smart contract di entrambe seguono il protocollo ERC-20¹ e hanno la stessa struttura; con il costruttore, al momento del deploy, vengono inseriti i seguenti parametri iniziali:

¹Protocollo: <https://github.com/ethereum/EIPs/issues/20>

- nome;
- simbolo;
- decimali (solitamente 18);
- quantità iniziale di token che vengono assegnati all'owner per poi essere distribuiti;

Nel contesto della gara i nomi e i simboli hanno le iniziali dei partecipanti e la quantità iniziale di Token è il 5% del valore iniziale presente nella propria pool, mentre quella di Paycoin ammonta a 50000 per tutti e tre i partecipanti (+5000, dati dal 5% dei Paycoin nella pool di ognuno). I decimali rappresentano le cifre dopo la virgola utilizzate per fare i calcoli negli smart contracts, in quanto Solidity ammette solo l'utilizzo di numeri interi positivi.

Una volta pubblicato, il contratto permette di eseguire le seguenti operazioni fondamentali:

- funzione di *minting*: un indirizzo, a cui è stato dato il permesso dal creatore, può creare nuovi token da zero e trasferirli ad un secondo ente;
- funzione di *transfer*: un indirizzo invia dei token ad un secondo indirizzo;
- funzione di *transferFrom*: un indirizzo invia dei token di un secondo indirizzo, dopo averne ottenuto il permesso tramite l'operazione di *approve*, ad un terzo indirizzo.

4.1.2 Pool

La Pool è il cuore dell'exchange dove avviene la compravendita dei Token, scambiati con Paycoin; nel nostro caso seguendo la regola del prodotto costante tra la quantità di Token e di Paycoin: $xy = k$.

Il suo costruttore accetta come parametri gli indirizzi del contratto Token a cui è associata e quello del contratto Paycoin, mentre al suo interno vengono inizializzate altre variabili utilizzate in seguito dalle funzioni.

Una volta pubblicata, la Pool è inizialmente vuota, perciò è presente la funzione *mint-liquidity*, utilizzabile una volta sola, che permette all'owner di inserire i valori iniziali di Token e Paycoin. La gara prevede tre tipologie di Pool, in base alla loro liquidità iniziale:

1. Pool con 100 Token e 100000 Paycoin;
2. Pool con 10000 Token e 100000 Paycoin;
3. Pool con 10000000 Token e 100000 Paycoin;

La Pool esegue due operazioni principali: *buy* e *sell*.

Il *buy* accetta come parametro il numero di Token x' che un utente vuole comprare e, tramite due funzioni di *transfer*, richiamate dai contratti Token e Paycoin, prende prima i Paycoin y' dal wallet dell'utente e poi consegna i Token comprati; i Paycoin vengono calcolati automaticamente con la seguente formula per mantenere k costante:

$$y' = \frac{k}{x - x'} - y$$

dove x e y sono i Token e i Paycoin contenuti nella Pool prima della transazione.

In realtà k varia leggermente, per via delle approssimazioni causate dal fatto che Solidity lavora solo con gli interi positivi. Inoltre, all'utente vengono prelevati ulteriori Paycoin che vengono

trasferiti direttamente all'owner della pool, dati dalle *fee* (commissioni) da pagare durante la transazione; le fee ammontano allo 0,3% dei Paycoin calcolati.

Il *sell* funziona al contrario del *buy*: l'utente inserisce il numero di Token che vuole vendere e riceve i Paycoin necessari a mantenere costante k , meno le fee, che vengono sempre trasferite direttamente all'owner.

Queste due operazioni vanno a modificare il prezzo, che è un valore indicativo di quanti Paycoin costa un Token, calcolato come rapporto tra la quantità di Paycoin nella pool e la quantità di Token; più si compra e più il prezzo sale, più si vende e più il prezzo scende. Ogni partecipante può comprare e vendere dalle pool degli avversari, ma non dalla propria.

Durante la gara i partecipanti possono aggiungere o togliere liquidità alle proprie pool, mantenendo, però, il contenuto di Token nella pool superiore al 50% del valore iniziale e inferiore al 150%; per questo sono presenti altre due funzioni utilizzabili solo dall'owner:

- il *mint-stake*: accetta come parametro il numero di Token da aggiungere nella pool, preleva direttamente dal wallet dell'owner questo ammontare di Token insieme ai Paycoin necessari per mantenere costante il prezzo, e aggiorna il valore di k ; è importante che questa operazione non sfori i limiti superiore e inferiore della pool: quindi, se per esempio la liquidità è in deficit l'owner deve inserire una quantità sufficiente da rientrare nel limite del 50%, altrimenti l'operazione fallisce;
- il *burn-stake* funziona al contrario: l'owner preleva Token e Paycoin dalla pool; questa operazione è molto vantaggiosa nel caso in cui la pool sfora sopra il limite superiore, in quanto permette al proprietario di guadagnare Paycoin, riportandola sotto il limite.

Sono presenti altre funzioni che prendono visione dei valori per monitorare l'andamento della Pool e una funzione utilizzabile una volta al giorno, detta *day-mint*, con la quale l'owner può mintare il 10% dei Token presenti nella sua Pool, moltiplicati per il numero del giorno della gara.

Tutte queste operazioni sono state temporizzate con un modificatore, in modo che si potessero eseguire solo negli orari di apertura del mercato previsto dalla gara, cioè dalle 9:00 alle 18:00, da Lunedì 17/07/2023 a Venerdì 21/07/2023.

4.1.3 Challenge

Per rendere la gara più avvincente è stato implementato anche un sistema di challenge molto semplice, realizzato con un apposito smart contract.

Il contratto offre 4 operazioni:

- lancio di una challenge singola;
- lancio di una challenge doppia;
- chiamata del contratto per la challenge singola;
- chiamata del contratto per la challenge doppia;

I lanci della challenge accettano come parametro d'ingresso l'indirizzo o gli indirizzi degli avversari che vengono sfidati, trasferisce allo sfidante 1000 Paycoin per la singola e 2000 per la doppia, come premio per averla lanciata, e viene emesso in rete l'evento del lancio della challenge; durante la gara, ogni partecipante deve far partire almeno 4 challenge e può lanciarne massimo 10 per tipo.

Una volta lanciata una challenge, bisogna aspettare 20 secondi e poi possono essere chiamate le funzioni per vincere la challenge: queste possono essere chiamate una sola volta e il primo che le chiama vince; a questo punto, il contratto trasferisce al vincitore 10000 Paycoin nel caso della challenge singola e 50000 per la doppia.

4.2 Bot e scripts

Per simulare un mercato reale sono stati creati 100 bot, che corrispondono ad un pubblico che compra e vende, creando un rumore nella variazione dei prezzi dei Token.

Per far ciò è stato creato prima un quarto account a fare le veci di admin: gestiva i bot, il contratto Paycoin e il sistema di monitoraggio delle pool.

I bot sono stati generati con degli indirizzi casuali a cui sono stati associati le loro chiavi private, utilizzate in seguito per aggiungerli in console; in seguito sono stati trasferiti loro degli Ether, accumulati dai partecipanti nelle settimane precedenti la gara, per permettere loro di fare transazioni in rete (quando si effettua una transazione viene pagata una fee in Ether ai miner, che confermano la transazione prima di essere aggiunta al blocco). Ai bot sono stati assegnati anche dei valori iniziali di Paycoin, estratti casualmente tra 1000 e 100000, secondo una distribuzione di probabilità uniforme.

Una volta distribuiti gli Ether e i Paycoin iniziali, i bot sono pronti per effettuare operazioni; il loro funzionamento avviene tramite uno script in Python e prevede un ciclo infinito che si rinnova ogni minuto, nel quale viene preso un bot casuale che compra e vende dalla medesima pool, anch'essa casuale. Il valore dei Token comprati o venduti dal bot viene scelto tra 0 e i Token massimi acquistabili o vendibili dal bot stesso e, prima dell'operazione, viene fatto un'*approve* dei token/paycoin che la pool può prendere dal bot, dovendo essa chiamare la funzione *transferFrom*.

In aggiunta allo script dei bot, sono stati scritti dei codici per agevolare l'interazione dei partecipanti con la rete tramite funzioni importabili all'interno della console, per effettuare le operazioni di inizializzazione dei contratti, *buy* e *sell* nelle pool avversarie (facendo in automatico le operazioni di *approve* necessarie), per monitorare le liquidità e i prezzi nelle pool e per monitorare i bilanci in Token e Paycoin di sé stessi e degli avversari. Queste ultime operazioni sono state eseguite anche in uno script di monitoraggio globale, che ogni mezz'ora salvava su un file di testo gli andamenti delle pool e dei bilanci nei wallet dei partecipanti.

Un ultimo codice non meno importante è quello delle challenge, che contiene le funzioni per lanciarle e chiamarle, più una funzione di monitoraggio che controlla gli eventi nella blockchain e avvisa tramite un bot di Telegram quando uno dei partecipanti è stato sfidato.

5 Analisi dell'andamento della gara

In questa sezione analizziamo l'andamento della gara. Anzitutto, ci concentriamo sull'andamento dei prezzi dei Token nelle pool e sul valore totale nei wallet di ogni partecipante, dati raccolti grazie al sistema di monitoraggio implementato. Indichiamo i tre Token con i loro simboli: DA (Token di Daniele), PB (Token di Paolo) e GR (Token di Giovanni); mentre i Paycoin hanno il simbolo PC.

5.1 Andamento dei prezzi

Nei seguenti grafici mostriamo l'andamento dei prezzi dei Token nelle tre pool.

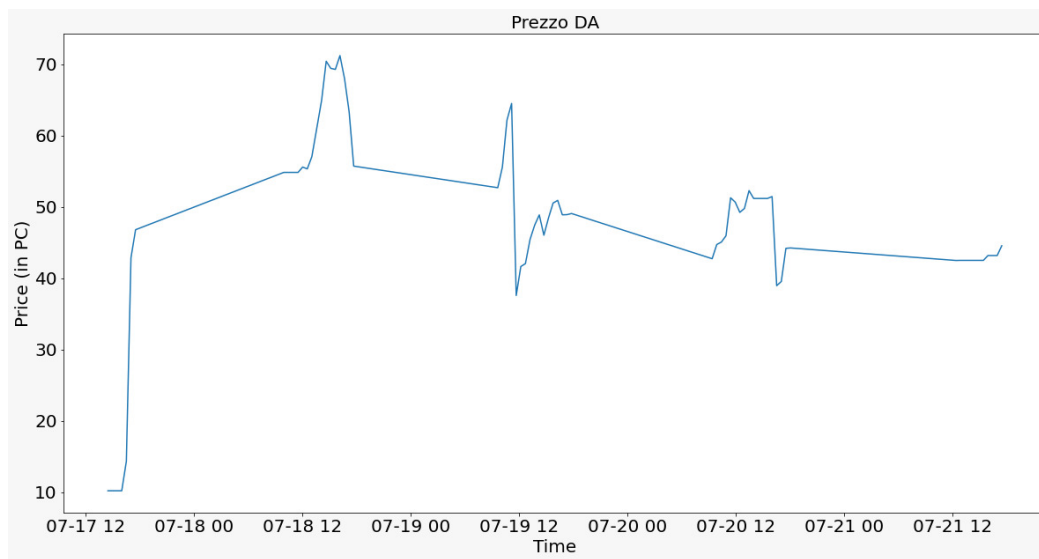


Figura 2: andamento del prezzo del Token DA.

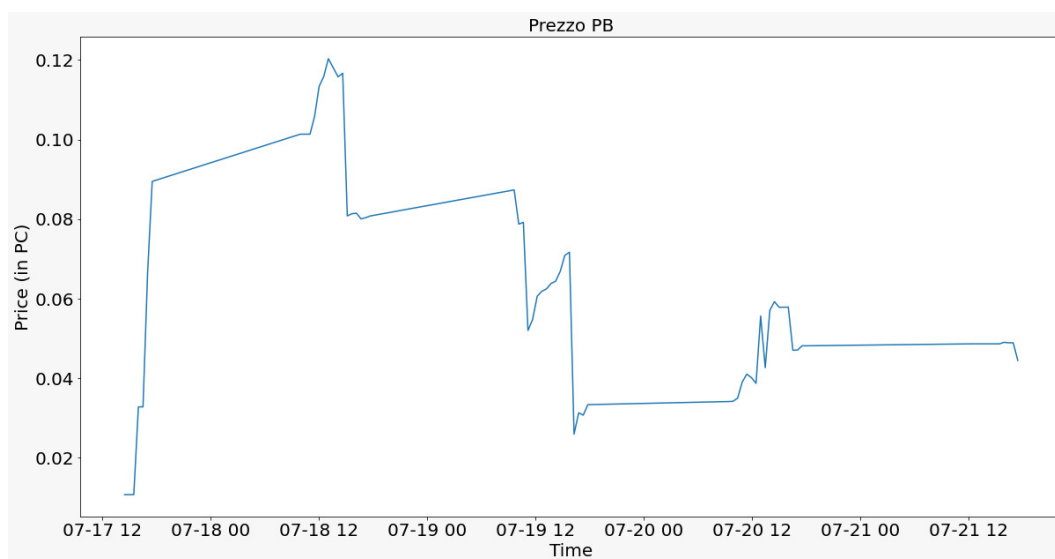


Figura 3: andamento del prezzo del Token PB.

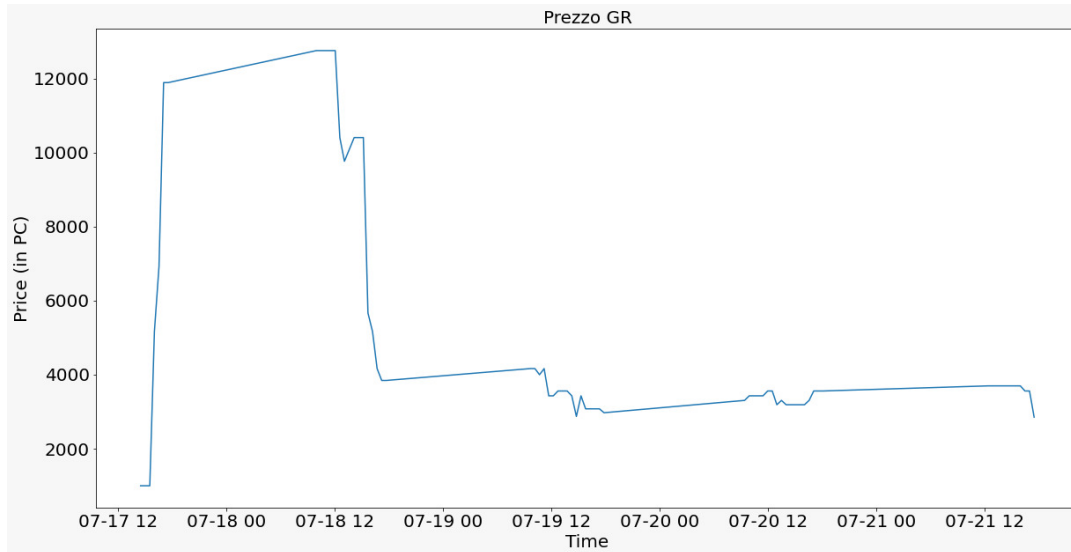


Figura 4: andamento del prezzo del Token GR.

Commentiamo i grafici.

- Il prezzo del Token DA, che partiva da 10 PC/DA, è cresciuto molto velocemente arrivando a 46.8 PC/DA nel primo giorno e 71.2 PC/DA nel secondo giorno; a questo punto, ad eccezione di una rapida oscillazione durante il terzo giorno nella quale è passato da 64.5 PC/DA a 37.6 PC/DA, ha iniziato una leggera discesa fino alla fine della gara, nella quale si è mantenuto tra 40 PC/DA e 50 PC/DA, arrivando al minimo di 39 PC/DA.
- Il prezzo del Token PB, che partiva da 0.01 PC/PB, è cresciuto rapidamente fino a 0.0895 PC/PB nel primo giorno ed è arrivato al picco di 0.1204 PC/PB nel secondo giorno, per poi discendere rapidamente fino a 0.0808 PC/PB, arrivando al minimo di 0.0260 PC/PB alla fine del terzo giorno; in seguito si è mantenuto tra circa 0.035 PC/PB e 0.055 PC/PB fino alla fine della gara, ad eccezione di una rapida oscillazione che l'ha portato fino a 0.0593 PC/PB.
- Il prezzo del Token GR, partendo da un valore iniziale di 1000 PC/GR, ha raggiunto il valore di 11890.6 PC/GR nel primo giorno e un picco di 12755.1 PC/GR nel secondo giorno, seguito da una rapida discesa fino a 4000 PC/GR; in seguito, il prezzo è rimasto relativamente costante tra 3000 e 3500 PC/GR, toccando il minimo di 2852.6 PC/GR.

Notiamo che per tutti e tre i Token c'è stata una rapida salita del prezzo durante il primo giorno (un fattore 5 per DA, 9 per PB e 12 per GR): questo è dovuto ad un malfunzionamento dei bot che, come verrà spiegato successivamente, durante l'inizio della gara hanno comprato molti Token senza rivenderne nessuno; a seguito del debug dello script dei bot, i prezzi sono ridiscesi, e, da quel momento in poi, non hanno mostrato ulteriori anomalie particolari, ma sono rimasti sottoposti semplicemente alle operazioni di trading dei partecipanti ed al rumore dei bot (effetti visibili nelle oscillazioni dei grafici). Tuttavia, l'effetto del bug iniziale dello script dei bot è stato così forte che i prezzi nel seguito della gara non sono mai scesi sotto il valore iniziale.

Possiamo anche osservare che il prezzo maggiormente soggetto ad oscillazioni è stato quello del Token PB, al contrario del token GR.

5.2 Wallet dei partecipanti

Analizziamo ora l'andamento dei valori nei wallet dei vari partecipanti. Il grafico seguente mostra l'andamento dei Paycoin nei wallet dei tre utenti.

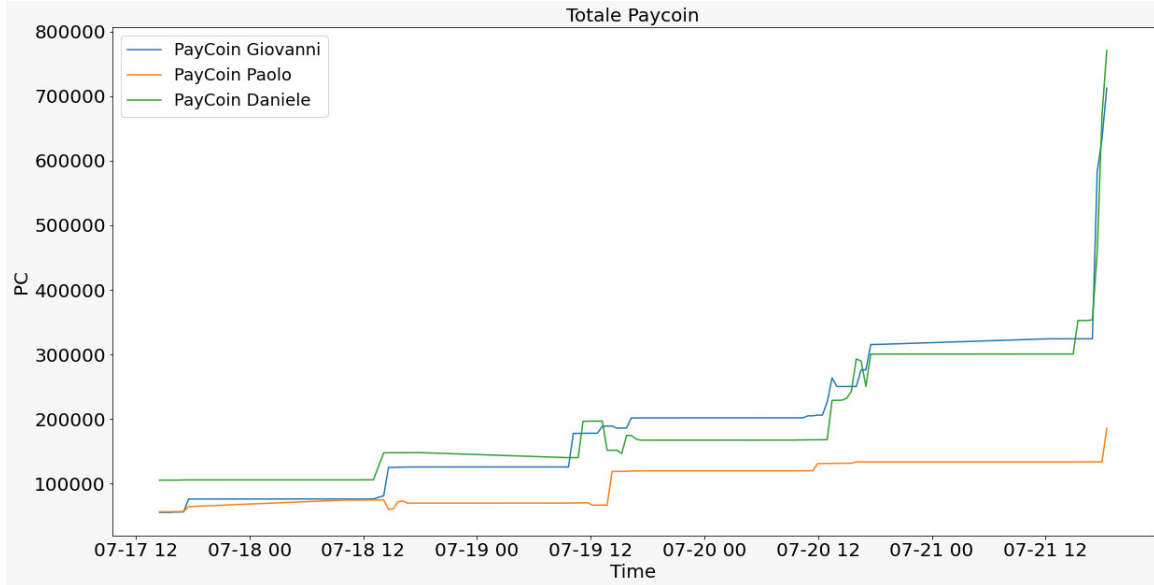


Figura 5: andamento del totale di Paycoin nei wallet dei partecipanti.

L'andamento per i tre utenti è qualitativamente simile: il trend è sempre in crescita, anche se vi sono alcune differenze. Paolo è sempre rimasto l'utente con meno Paycoin durante tutta la gara; nella prima metà Daniele possedeva più Paycoin di tutti, ma è stato superato da Giovanni nel terzo giorno. Notiamo che la crescita dei Paycoin nei wallet avviene con brusche salite, che sono dovute a vittorie nelle challenge; le oscillazioni meno ampie, invece, sono dovute a operazioni di trading, a volte efficaci, altre volte fallimentari. Non vi sono comportamenti particolarmente anomali, ma si può osservare una decisiva crescita dei Paycoin di Daniele e Giovanni alla fine della gara: in quel momento, infatti, hanno rivenduto tutti i Token in loro possesso, raccolto parte dei Paycoin contenuti nelle loro pool e lanciato numerose challenge nella ultima mezz'ora di gara. I guadagni dei tre giocatori in termini di Paycoin sono contenuti nella seguente tabella:

Utente	PC iniziali	PC finali	Variazione	Variazione percentuale
Daniele	55000	771082	+716082	+1302%
Paolo	55000	185407	+130407	+237.1%
Giovanni	55000	712726	+657726	+1196%
Totale bot	4826759	4544004	-282755	-5.86%

Tabella 1: Paycoin iniziali e finali dei vari partecipanti e del totale dei bot, variazione assoluta e percentuale.

Gli stessi dati, relativi ai singoli bot, sono riportati in Appendice. Dalla tabella concludiamo che tutti e tre i giocatori hanno guadagnato Paycoin durante la gara, anche se Daniele e Giovanni in misura maggiore rispetto a Paolo; Daniele è l'utente che ha concluso la gara con il maggior

numero di Paycoin nel wallet. I bot, invece, in media hanno perso Paycoin: questo è dovuto alle grosse quantità di Token che hanno comprato a inizio gara.

Nel seguente grafico sono riportati gli andamenti del valore complessivo dei wallet dei tre partecipanti: il valore complessivo è calcolato in Paycoin, sommando ai Paycoin presenti nei wallet i vari Token posseduti dall'utente moltiplicati per il loro prezzo *attuale*.

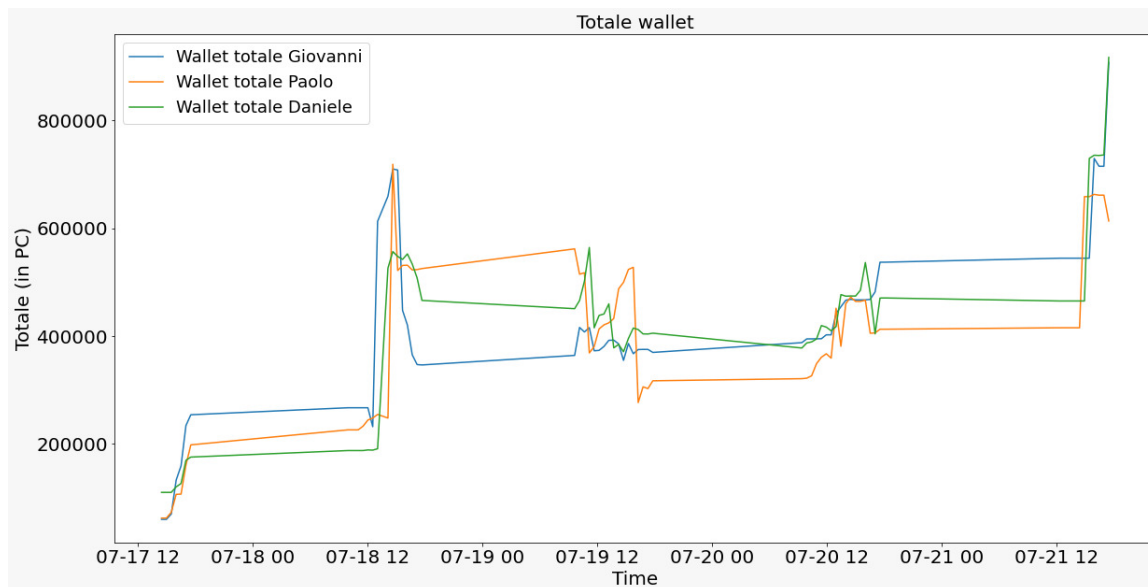


Figura 6: andamento del valore totale nei wallet dei partecipanti.

Osserviamo che vi sono diverse differenze rispetto all'andamento dei Paycoin. Anzitutto, le oscillazioni in questo grafico sono decisamente più marcate: questo avviene perché i valori nel grafico sono soggetti anche alle oscillazioni dei prezzi dei Token, oltre che alle variazioni dovute alle azioni di compravendita degli utenti; inoltre, la differenza tra i tre utenti non è così evidente come nel caso dei Paycoin: nel secondo e nel quinto giorno Giovanni ha maggiore ricchezza nel wallet, nel terzo giorno Paolo, mentre nel quarto Daniele. A fine gara, la ricchezza complessiva di Daniele e Giovanni è superiore rispetto a quella di Paolo, ma in maniera meno marcata rispetto a quanto si è osservato nel grafico dei Paycoin; tuttavia, occorre specificare che la ricchezza rappresentata in questo grafico è soltanto ricchezza virtuale: la ricchezza reale è rappresentata dai Paycoin, non dai Token, che, se non sono stati venduti entro la fine della gara, hanno perso completamente valore (in quanto non più scambiabili).

5.3 Swap effettuati

Nella seguente tabella riportiamo dei dati relativi all'attività di acquisto e di vendita nelle diverse pool:

Pool	n° <i>buy</i>	n° <i>sell</i>
Daniele	242	252
Paolo	241	212
Giovanni	212	220

Tabella 2: numero di operazioni di *buy* e *sell* registrate nelle tre pool.

In generale, non vi sono grosse differenze in merito ai numeri di swap fatti nelle tre pool: questo deriva dal fatto che le azioni dei bot erano completamente casuali. La pool di Daniele è stata quella soggetta a maggior attività di trading da parte degli utenti, seguita da quella di Paolo, e infine da quella di Giovanni. Noto è il fatto che, mentre nelle pool di Daniele e Giovanni la differenza tra i *buy* e *sell* è di ordine 10, nel caso della pool di Paolo risulta essere circa il triplo: questa, infatti, presenta circa trenta *buy* in più rispetto ai *sell*, e ciò potrebbe spiegare perché le salite del prezzo PB sono tendenzialmente più lente rispetto alle discese: questo, infatti, sarebbe l'effetto di molti *buy* di pochi Token e pochi *sell* di molti Token.

Nella tabella non sono presenti gli swap effettuati tra due diversi Token, in quanto un bug nell'impostazione dell'exchange ha reso questi impossibili, come verrà spiegato meglio nella prossima sezione.

5.4 Fee pagate

Nella seguente tabella riassumiamo il totale di fee pagate dagli utenti e dai bot:

Utente	Fee pagate (PC)	% sui PC iniziali
Daniele	312.21	0.5677%
Paolo	108.61	0.1975%
Giovanni	405.68	0.7376%
Totale bot	10530	0.2182%

Tabella 3: fee totali pagate dai singoli partecipanti e dal totale dei bot, percentuale relativa all'ammontare di PC iniziali (nel caso dei bot si calcola sul totale dei PC posseduti da tutti i bot).

Il valore delle fee pagate si mantiene sempre sotto l'1% dei Paycoin posseduti a inizio gara. La percentuale in tabella può essere indice dell'attività del giocatore: Giovanni risulta essere l'utente che in generale ha svolto più operazioni di trading, seguito da Daniele e da Paolo; i bot, in media, hanno avuto un'attività paragonabile a quella di Paolo.

5.5 Challenge

Come anticipato sopra, le challenge si sono rivelate il metodo più fruttuoso per gli utenti per guadagnare Paycoin. Nella tabella seguente riportiamo le statistiche relative alle challenge:

Utente	1v1 chiamate	1v2 chiamate	1v1 vinte	1v2 vinte	Paycoin guadagnati
Daniele	10	10	10	12	730000
Paolo	5	5	3	2	145000
Giovanni	10	9	9	10	618000

Tabella 4: statistiche relative alle challenge: numero di challenge 1v1 e 1v2 chiamate e vinte, guadagno totale in Paycoin.

Confrontando questi dati con quelli in Tabella 1, notiamo che sia Daniele che Paolo hanno perso circa 15000 PC con operazioni di trading (circa il 27,3% dei Paycoin iniziali): infatti, i Paycoin guadagnati per le sole challenge sono maggiori dei Paycoin totali guadagnati durante la gara; dunque, non solo il loro guadagno è dovuto alla vittoria delle challenge, ma questo ha anche riparatato le perdite fatte in trading; a differenza di Giovanni, il quale, oltre ad aver guadagnato

molti Paycoin con le challenge, ne ha guadagnati circa 40000 con operazioni di trading (circa il 72,7% dei Paycoin iniziali).

Nelle seguenti tabelle riportiamo dati più specifici in merito alle challenge lanciate.

Giorno	Tipo	Sfidante	Sfidato	Vincitore
1	1v1	Paolo	Giovanni	Giovanni
1	1v1	Paolo	Giovanni	Giovanni
1	1v1	Paolo	Giovanni	Paolo
2	1v1	Daniele	Paolo	Daniele
3	1v1	Giovanni	Paolo	Giovanni
3	1v1	Paolo	Giovanni	Paolo
3	1v1	Giovanni	Daniele	Giovanni
3	1v1	Daniele	Giovanni	Daniele
3	1v1	Daniele	Paolo	Daniele
4	1v1	Giovanni	Paolo	Giovanni
4	1v1	Paolo	Daniele	Paolo
4	1v1	Giovanni	Paolo	Giovanni
4	1v1	Giovanni	Daniele	Giovanni
5	1v1	Daniele	Paolo	Daniele
5	1v1	Daniele	Paolo	Daniele
5	1v1	Giovanni	Paolo	Giovanni
5	1v1	Daniele	Paolo	Daniele
5	1v1	Daniele	Paolo	Daniele
5	1v1	Daniele	Paolo	Daniele
5	1v1	Daniele	Paolo	Daniele
5	1v1	Daniele	Paolo	Daniele
5	1v1	Giovanni	Daniele	Giovanni
5	1v1	Giovanni	Daniele	/
5	1v1	Giovanni	Paolo	/
5	1v1	Giovanni	Paolo	/

Giorno	Tipo	Sfidante	Vincitore
1	1v2	Paolo	Daniele
3	1v2	Daniele	Daniele
3	1v2	Paolo	Giovanni
3	1v2	Giovanni	Giovanni
4	1v2	Daniele	Daniele
4	1v2	Paolo	Paolo
4	1v2	Giovanni	Giovanni
4	1v2	Daniele	Daniele
4	1v2	Paolo	Daniele
4	1v2	Giovanni	Daniele
5	1v2	Giovanni	Giovanni
5	1v2	Daniele	Daniele
5	1v2	Giovanni	Giovanni
5	1v2	Giovanni	Giovanni
5	1v2	Daniele	Giovanni
5	1v2	Daniele	Giovanni
5	1v2	Daniele	Daniele
5	1v2	Daniele	Daniele
5	1v2	Daniele	Daniele
5	1v2	Giovanni	Daniele
5	1v2	Giovanni	Paolo
5	1v2	Giovanni	Daniele
5	1v2	Paolo	Giovanni

Tabella 5: statistiche relative alle challenge 1v1 (a sinistra): giorno, sfidante, sfidato e vincitore; statistiche relative alle challenge alle challenge 1v2 (a destra): giorno, sfidante e vincitore (gli sfidati sono sottintesi). Notare il numero di challenge lanciate nell'ultimo giorno.

Notiamo che le ultime tre challenge 1v1 non hanno nessun vincitore: questo perché le ultime challenge sono state lanciate in massa nei momenti finali della gara e, essendosi sovrapposte una all'altra, non tutte hanno ricevuto la chiamata che ne avrebbe decretato il vincitore.

6 Problemi e anomalie

Durante lo svolgimento della gara sono stati riscontrati alcuni problemi legati a bug dei contratti e degli scripts, che hanno alterato in misura non trascurabile l'andamento della gara.

6.1 Funzionamento dei bot

L'anomalia che ha avuto un impatto maggiore è legata al funzionamento dei bot. Come anticipato sopra, lo script dei bot presentava un problema cruciale: nella mattina del primo giorno, ossia all'avvio della gara, i bot hanno iniziato ad acquistare in massa grosse quantità di Token dalle pool, senza rivenderli; questo era legato alla modalità con cui venivano estratte casualmente le operazioni fatte dai bot: a inizio gara, infatti, i bot non avevano alcun Token nei wallet, e, poichè il codice non teneva conto di questo fatto, la probabilità di rivendita era molto minore rispetto alla probabilità di acquisto di un Token. Il problema è stato prontamente risolto con una rapida modifica dello script, ma, come spiegato prima, ha avuto effetti tutt'altro che trascurabili sull'andamento dei prezzi durante tutta la gara. Occorre specificare che era del tutto normale che all'inizio i bot acquistassero Token: il problema è nato nel momento in cui le quantità acquistate, dopo aver modificato notevolmente la liquidità delle pool, non venivano rivendute e ciò ha avuto grossi effetti sul mercato, mentre l'obiettivo dei bot doveva essere soltanto quello di creare rumore di fondo.

6.2 Funzioni di minting

I contratti delle Pool e gli scripts per il loro utilizzo avevano dei bug importanti nelle funzioni *day-mint* e *mint-stake*:

- a causa di un errore nell'impostazione delle condizioni temporali, la funzione *day-mint* è risultata inutilizzabile nel terzo e nel quarto giorno della gara;
- per un problema legato all'approssimazione dei valori nel passaggio tra Python e Solidity, gli *approve* chiamati per la funzione di *mint-stake* potevano risultare insufficienti; per risolvere questo malfunzionamento, era necessario aggiungere un intero in più al valore di cui veniva fatto l'*approve*.

6.3 Swap

Nell'exchange realizzato, l'owner di una pool non poteva comprare e rivendere i propri Token, ma poteva scambiarli con Token altrui, tuttavia questa cosa non è stata possibile per un errore nell'impostazione del sistema: la funzione di *swap* tra due Token, infatti, è stata implementata negli scripts, e richiedeva le pool come intermediarie dello scambio: se, per esempio, un utente avesse voluto scambiare dei Token 1 per dei Token 2, la funzione avrebbe venduto i Token 1 alla Pool 1 e comprato, con i Paycoin ricevuti, un certo ammontare di Token 2 dalla Pool 2; appare chiaro, ora, come sia impossibile chiamare la funzione se uno tra Token 1 e Token 2 è il proprio Token. Questo è stato un errore grave, in quanto la ricchezza rappresentata dai propri Token poteva essere sfruttata soltanto per operazioni di *mint* e *burn* nella propria pool. Inoltre, per come era impostata la funzione, fare gli swap possibili (quindi tra i due Token non propri) è risultato dispendioso in Paycoin e i partecipanti hanno preferito fare operazioni di trading solo comprando e rivendendo direttamente alle pool. Una soluzione a questi problemi poteva essere la

presenza di un terzo contratto che, chiamato dall'utente, avrebbe interagito con le pool e fatto le operazioni di swap.

6.4 Lentezza della rete

Vi è, infine, un ultimo problema, non dovuto a bug o errori di programmazione. Soprattutto negli ultimi due giorni, gli utenti hanno riscontrato problemi legati alla lentezza della rete: le transazioni lanciate sulla blockchain, infatti, sono arrivate a richiedere addirittura qualche minuto per la conferma, rendendo di fatto estremamente lenta qualsiasi operazione; questo probabilmente era legato al fatto che la quantità di gas pagato per le transazioni era troppo bassa e quindi queste avevano bassa priorità nella blockchain. L'impatto maggiore di questo fattore è stato visibile nelle challenge: in condizioni di velocità normale, era molto probabile che a vincere una challenge fosse colui che l'aveva lanciata; mentre, in questa situazione, ciò non era più valido, in quanto le operazioni di chiamata della challenge venivano confermate con tempistiche più lunghe, a volte sufficienti per dare la possibilità allo/agli sfidato/i di rispondere in anticipo.

Concludiamo osservando che questi bug non si prestavano ad essere sfruttati dagli utenti per aggirare il sistema e guadagnare in maniera illecita, ma piuttosto hanno rappresentato un fattore di limitazione per tutti i partecipanti.

7 Conclusioni

In questa relazione abbiamo descritto e commentato la realizzazione e l'utilizzo di un exchange decentralizzato finalizzato ad una gara di trading tra i tre autori del progetto.

Nonostante alcuni problemi iniziali, la gara è proceduta in maniera abbastanza liscia, se non per alcuni problemi e limitazioni che gli utenti hanno incontrato. Durante l'inizio della gara, i bot hanno comprato numerosi Token, aumentando drasticamente i prezzi e diminuendo le liquidità delle pool; dopo aver sistemato lo script dei bot, i parametri si sono ristabiliti relativamente vicino ai valori iniziali, lasciando la libertà ai partecipanti di fare normali operazioni di trading, nonostante le limitazioni imposte da altri bug nei contratti e negli script (*mint-stake* mal funzionante e alcuni *swap* non possibili).

La gara si è mostrata interessante, anche se è risultato evidente che i partecipanti non fossero dei trader esperti: due dati notevoli, in effetti, sono il fatto che il guadagno finale è dovuto alla vittoria delle challenge e il fatto che due giocatori su tre sarebbero andati in perdita in assenza di queste.

8 Appendice

In Appendice è possibile consultare alcuni grafici e tabelle con dati interessanti, non riportati nelle sezioni precedenti per motivi di spazio.

8.1 Andamento dei Token nei wallet dei partecipanti

Nei seguenti grafici sono riportati gli andamenti dei diversi tipi di Token contenuti nei wallet dei partecipanti.

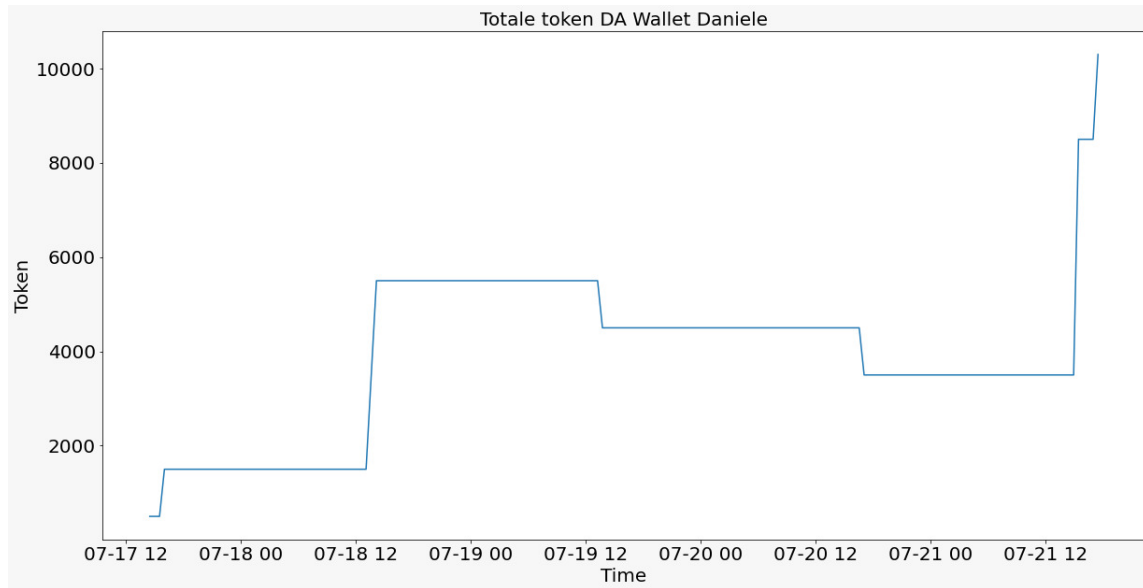


Figura 7: andamento del totale di token DA nel wallet di Daniele.

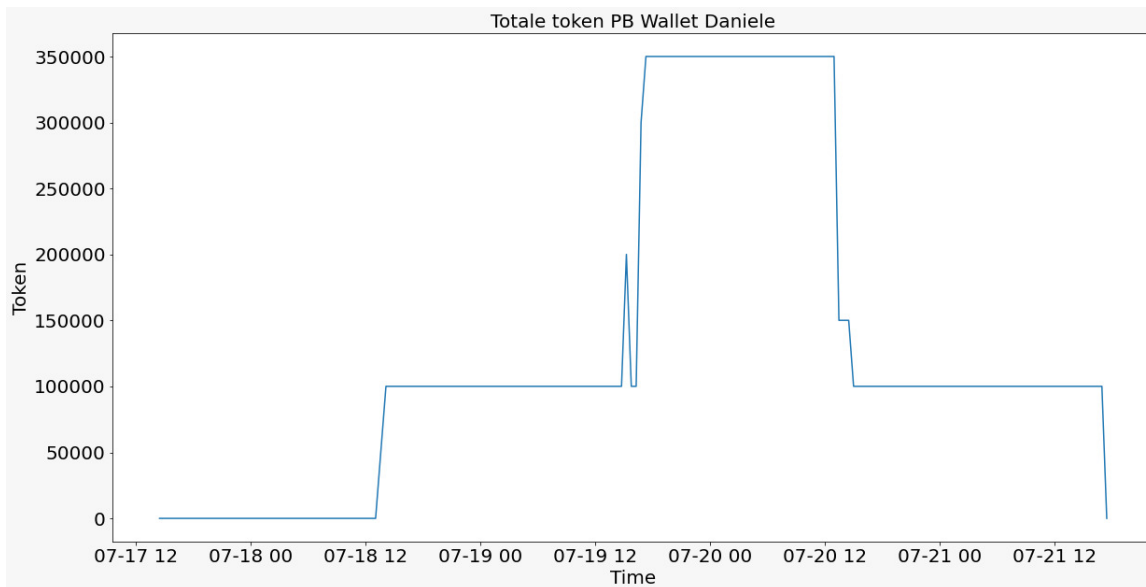


Figura 8: andamento del totale di token PB nel wallet di Daniele.

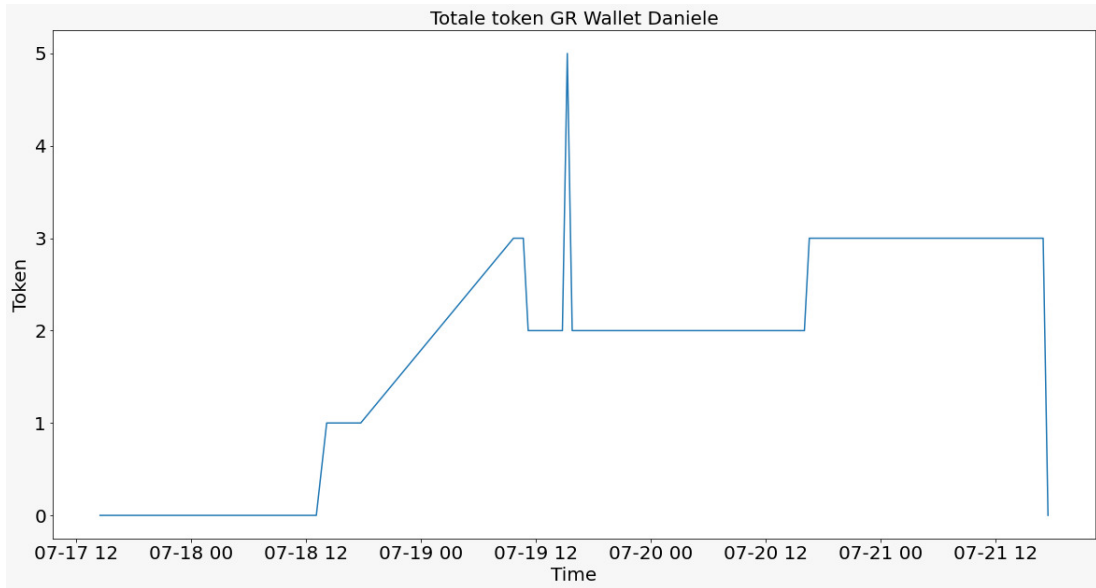


Figura 9: andamento del totale di token GR nel wallet di Daniele.

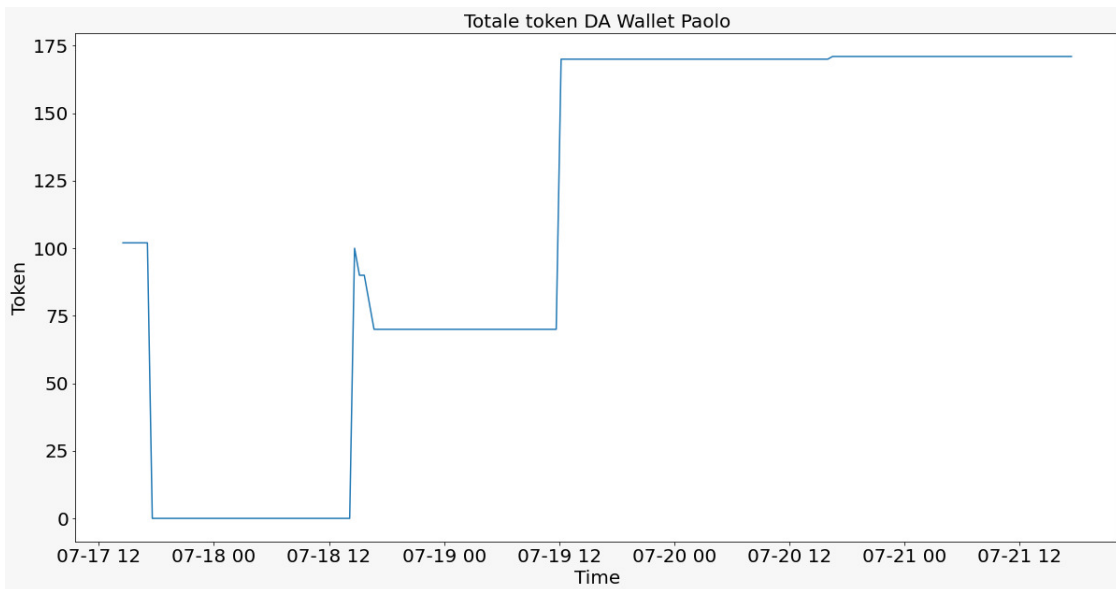


Figura 10: andamento del totale di token DA nel wallet di Paolo.

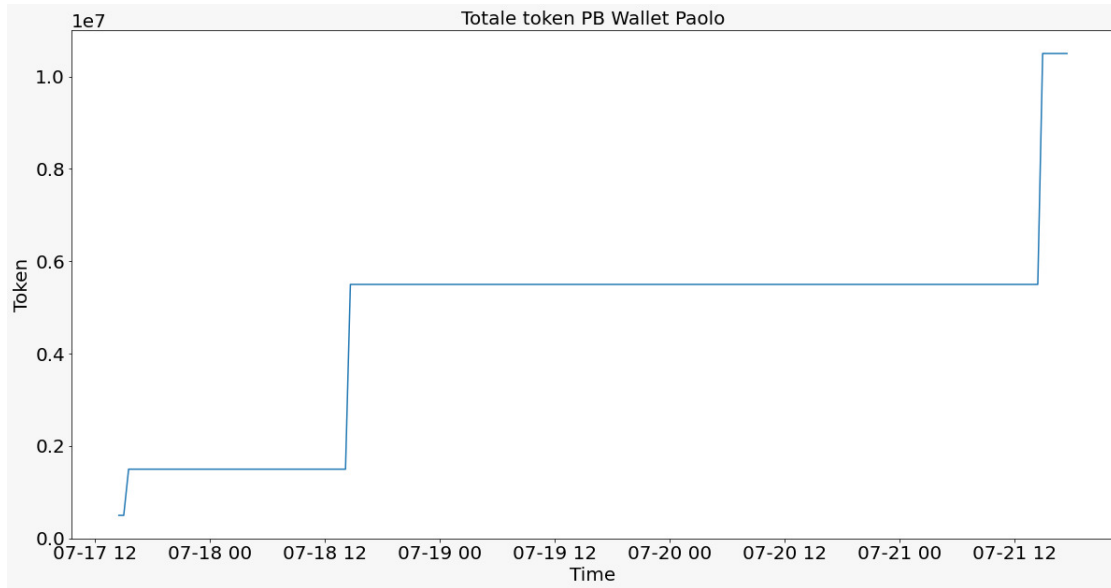


Figura 11: andamento del totale di token PB nel wallet di Paolo.

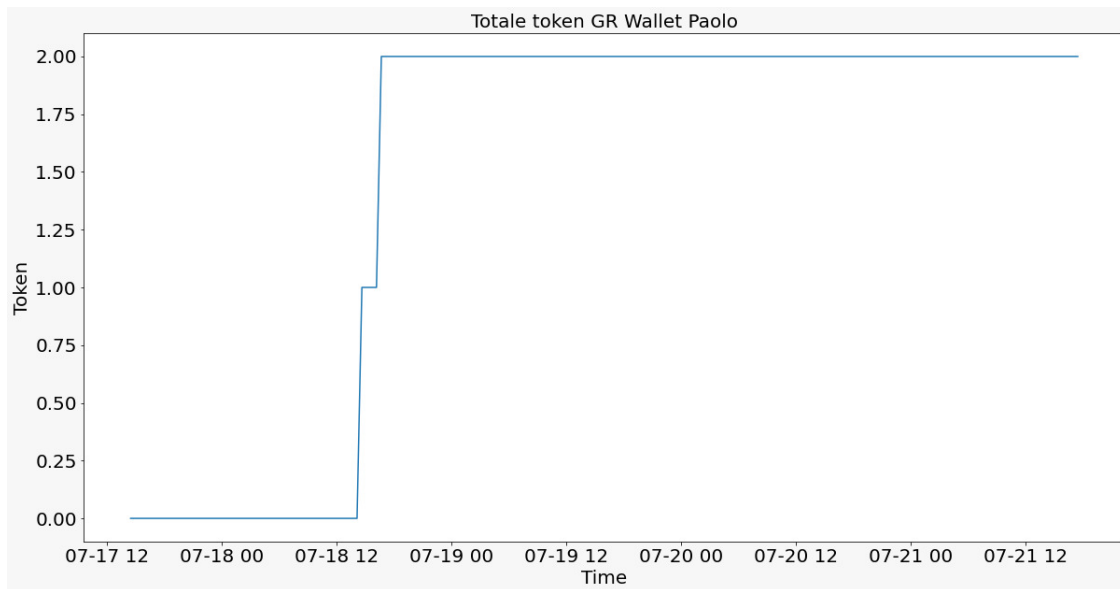


Figura 12: andamento del totale di token GR nel wallet di Paolo.

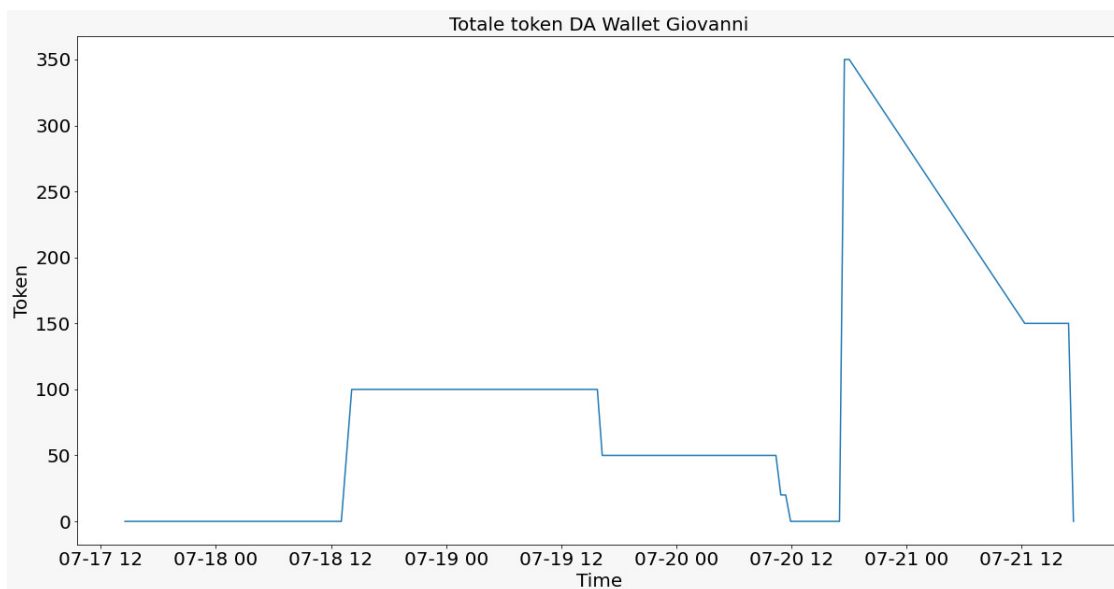


Figura 13: andamento del totale di token DA nel wallet di Giovanni.

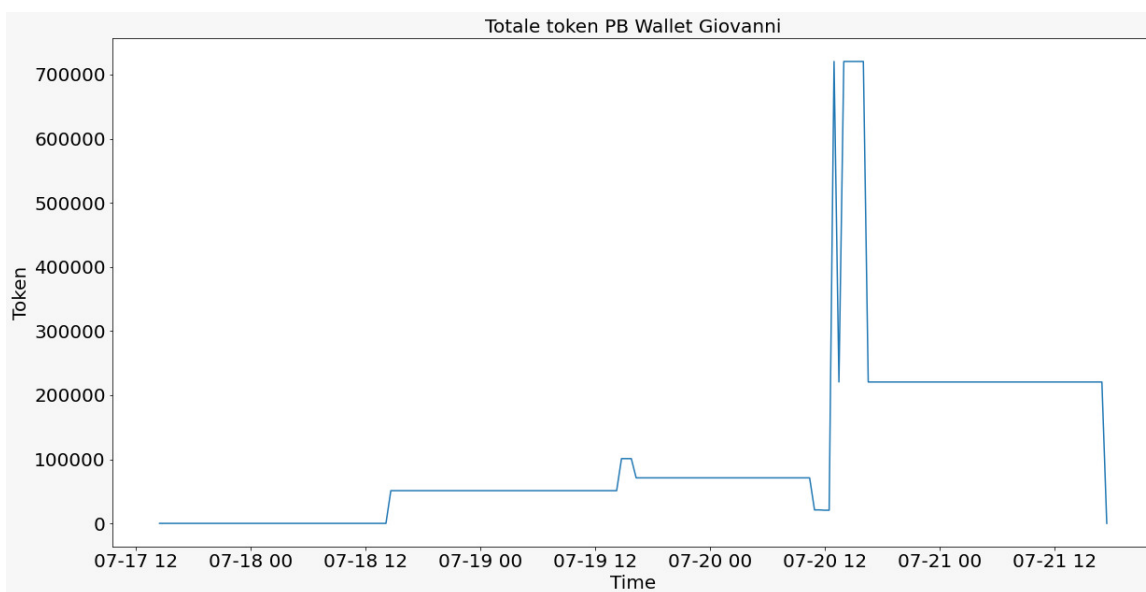


Figura 14: andamento del totale di token PB nel wallet di Giovanni.

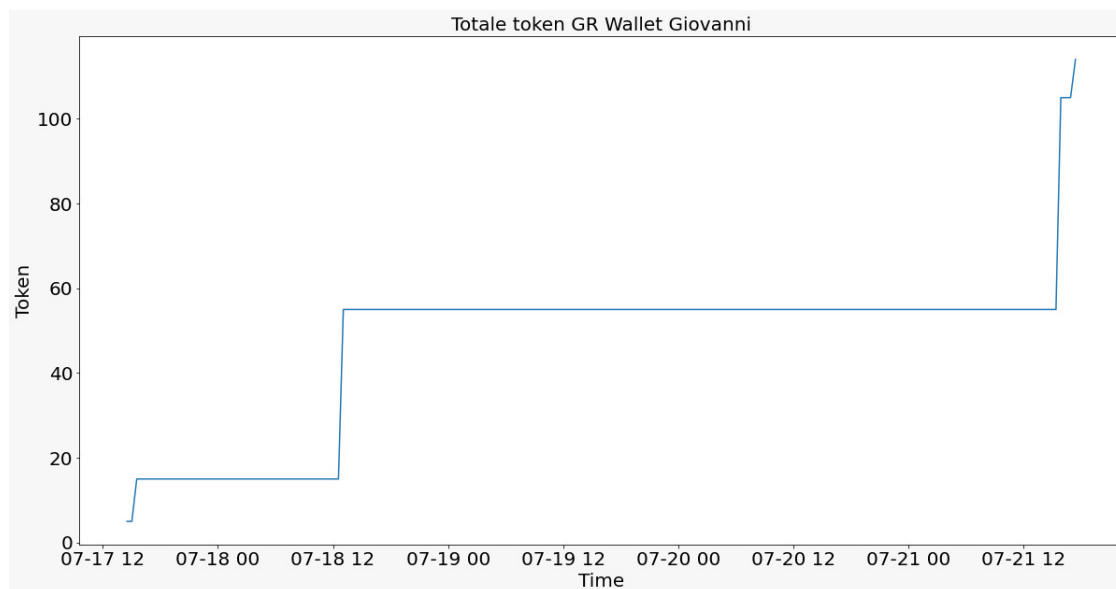


Figura 15: andamento del totale di token GR nel wallet di Giovanni.

8.2 Dati sui singoli bot

Nelle seguenti tabelle, riportiamo i dati relativi al guadagno/perdita in Paycoin e al pagamento in fee per ogni singolo bot utilizzato nella gara.

Indirizzo bot	PC iniz.	PC fin.	Var.	Var. %
0x5392927A750499B27C140ba843b2ca30F5F0E2a4	42916	37889	-5026	-11.71%
0xe2Ea05a1FC8a522C78fA7A3561F455fb8e6Ee708	88679	143546	54867	61.87%
0x7e354aA981B6dbE3C66037033152c86FA68518C3	67384	64953	-2430	-3.6%
0x99d06632445AfAc088A7E6050A6747aa01f744d5	78666	73426	-5239	-6.66%
0x012Ed6cC8A5F4E0A26defeADbFb7b365C2d55060	77562	67297	-10264	-13.23%
0x0F27B686873b17BB8DE85e3F3268d2b402A2819f	85046	72191	-12855	-15.11%
0xfBA6c71B68Ab867e03ECA385D65a60B385720FfC	3326	3027	-298	-8.96%
0x3FC1168d4EC8511d92D46A907E50509584b41e9f	67735	63574	-4160	-6.14%
0xb71a10753da50d4Dc8e78B603342B7F5465D7415	38495	35977	-2517	-6.53%
0x4F76743E6C975Bab7D46b8Aefc99802231F9FD08	78818	77344	-1473	-1.86%
0x6C9BA7A6Ffeb5Ffa1bFBaC31325438812bE770a9	24917	22732	-2184	-8.76%
0xE9C23E1f4dF8b934a218d2ac497ee28AE680f649	10779	8584	-2194	-20.36%
0x7252B9276d057842970A882a1328dc08917006B4	47983	46018	-1964	-4.09%
0xe01667456C2fa6A2dF68525C39a85A155B84B093	96476	83310	-13165	-13.64%
0xb2Dc0ac6406193B546DEc16acFb08ecD13D08584	3800	3836	36	0.96%
0xaE4bF961fB2b51870047D44Bac95Bd6e400A426	2321	2212	-108	-4.68%
0x4D09b13a42393f4cf2147666f1461EF68471866A	19714	18990	-723	-3.67%
0x5bD6C66b42Cd58583079a3552663Fb49a7A78A1D	55446	49570	-5875	-10.59%
0xbC8511E3a7098CD394A368a04801c3390BE61bE4	50216	41819	-8396	-16.72%
0x766dF54e7ccDec373410FEbc7Fcac14dC4a2bF3A	51258	28227	-23030	-44.93%
0x563cFc69DE81627d26F82802317b753741c4B52b	33877	32584	-1292	-3.81%
0x74BE597A72EF4e4Ff3313C05bFcaaA7f961bC09B	65304	64096	-1207	-1.84%
0x384D9e3F1Fae476a79e3152784Db56B2a374c280	84435	76044	-8390	-9.93%
0x225c651D54B4021793B03EE0A74d354343e6ca98	24275	23010	-1264	-5.21%
0x5627b9874BeDC9dc27f92908E384171678c8FfCd	8603	19586	10983	127.67%
0xB9F1c48A333c176634803aefb2c11450Bf11E5ef	59313	63425	4112	6.93%
0xE067d75A81eB2Bc1b9C8BBed919a370fE46c631B	40966	33371	-7595	-18.53%
0xEdbD8723FcF67a4D675726a034c11C9A81E22a63	30798	27753	-3044	-9.88%
0x228762d14e93A9bB5e9B4F69D3f4bd55657aa3B6	46546	42851	-3694	-7.93%
0xcF313B3Ebc584a2596C9f1ff352cD6215FBc84f2	11651	9385	-2266	-19.45%
0x158DBD55cc67C54E43459894C4d4f4E9F566D3E3	43900	41389	-2510	-5.71%
0x1A6a254aFE9b9b65aEcd1c9EA04E7521da03186E	21738	16730	-5007	-23.03%
0x1Af5F9152A833ff2d30585536EC6421A7Df2BF4d	34452	28741	-5710	-16.57%

Tabella 6: dati per i primi 33 bot: Paycoin iniziali e finali, variazione assoluta e percentuale.

Indirizzo bot	PC iniz.	PC fin.	Var.	Var. %
0x2EF92db880e619701c15177F710bC107720aBa11	95312	82885	-12426	-13.03%
0x88e18973562d2F22E6138938035E0eB0f96578fC	24044	20892	-3151	-13.1%
0xe08B1925201E5A5FA2BfAC6A2E5f348E4dba19B8	11443	10357	-1086	-9.49%
0xe71D0C2059Ad76497D3697f24961f5E81d61F039	82045	76314	-5730	-6.98%
0x7b3B037345cA2F878687fdA8D8f3A6580E436Bd3	82352	77637	-4714	-5.72%
0x701D54b96d88f8077feEc2C15a5BeF7D1E6cb202	3791	3689	-101	-2.67%
0x6B3F9874b4b13Dac5e4d8182374B0aD20Cf0a5d2	9942	9153	-788	-7.93%
0xec23b31f616D96c95cdc2F32D9225dA47d695d1F	17782	17365	-416	-2.34%
0x48fCC9ccA03f0476455c3291b4Af71aD8E4bbd2e	77950	67049	-10900	-13.98%
0x060fcfF0F88ae5D33367c8b4139d64E2277cC0d4	28827	25796	-3030	-10.51%
0xeC557115C7A0e9347d56566043D9B9B847d25dec	27233	25455	-1777	-6.52%
0x8B9540D8ea478CdEB736e1f5F82E566EfD1342c8	76258	57644	-18613	-24.4%
0x33035ED633A3cED9005Ece48CF65f164B430199C	69967	87384	17417	24.89%
0xfDf0b19f842f564D309a351E1eDC5250f06e7b3B	48454	52228	3773	7.78%
0x380351dC5Ebd4aC5117cA7b8F2343b97B3C03e0b	97935	93654	-4280	-4.37%
0x63B697a6D43C37d2B24f32a6303B57B5DD5D47ef	87628	102265	14637	16.7%
0x45E2E2B28EfC9f3890F7411CBbF0F4fa5E84E066	69031	74305	5274	7.64%
0xA73A8Ad1add220dfFcE68BACe1E89a6481E7fdCF	91416	81018	-10397	-11.37%
0xd82bDeAc4dc8Ad2858aCB82eb03f2Dd949991d16	12051	9201	-2850	-23.64%
0x6BF3dDa6FF3C67AC3b35C102fb68cBe8899059Be	53399	35032	-18366	-34.39%
0x48F041F1b2408E9b0A762907626Ea056BC70fE9A	38214	32952	-5261	-13.76%
0x2D242ACd72f1199177BAA71bC099Dba2BBE2ed3f	38067	33735	-4331	-11.37%
0xEcFBe2844093e016717324429459E480213c29c9	16714	15005	-1708	-10.22%
0x6789b513c7483c35232Bb084d5245E5aDDE58206	45953	44695	-1257	-2.73%
0xcb5AE51F1F145626E49e54cEbFD8943692Aa8020	68838	50833	-18004	-26.15%
0x0Dab9E319fb3756197E867b6014b107284Ef95E7	16140	19409	3269	20.25%
0x117A3642e3407856eC5223Fc1AF22Ec9A4B85B2B	66953	56790	-10162	-15.17%
0x472C53d0BBEC2efAEFcAFE1969BD1668a3161C9f	62484	50628	-11855	-18.97%
0xad3d3011c58E47339795BdA8c9A478d71d6f75d2	90216	78585	-11630	-12.89%
0x52ecfE54606b8a705afA046cFF74cf7FAD415a9D	17090	16639	-450	-2.63%
0xDd6AD0fb33Ffe17DBE2822409A9073a674e88926	96728	88086	-8641	-8.93%
0xa2CA083d008d9A59E22eBa3B6f64714bf816c110	93754	80121	-13632	-14.54%
0x1d2Cbcce57207053375F70Ef28E405f605dEf2051	87064	74755	-12308	-14.13%

Tabella 7: dati per i bot dal 34° a 66°: Paycoin iniziali e finali, variazione assoluta e percentuale.

Indirizzo bot	PC iniz.	PC fin.	Var.	Var. %
0xC280370BCcDcf9D918767ccC158c8dF53dB2D2e7	69850	58825	-11024	-15.78%
0x6B943c96FeF8845A2Fff7a9aBCaC82db0a6F0c9D	90521	86949	-3571	-3.94%
0xdB6485c575781bBeF3F79EDFC85D246DaE2BA8Ba	43791	42039	-1751	-4.0%
0xF71C4A52a5ae9dd1fBd30670c6310c423E7f78F5	18993	15197	-3795	-19.98%
0x048421bFf43B016439B35684e69C54dCC581526D	59935	56466	-3468	-5.78%
0x3c83f996b9A898aff6A41Ff8b03AE05d2DF08871	76137	71915	-4221	-5.54%
0xD44e43CaE6e51D64a48e781756D1F05eeF0e3b2F	56125	50251	-5874	-10.46%
0xdb8b0217c5089784eb49D84763f8bc82365e8726	5615	5012	-602	-10.72%
0x2845867f16C77771dCC61B855E4312CcAAc64878	43769	65016	21247	48.54%
0xee6bd0A5f5287eC909F30ca5180f35da00632440	38077	31756	-6320	-16.59%
0x4f209Ee52FcB45C1B47302a4299fe30E9B9D8aDC	81705	68056	-13648	-16.7%
0x07DA069d0902649Df096e53185c3626e9469Aaf6	41435	34630	-6804	-16.42%
0xB89b7Cc588D998602cC283C67a4b9e8F1F4859db	66204	60555	-5648	-8.53%
0x32eAdeB7A1c8310fa31b417ea8E862eBa5d6475C	25581	24933	-647	-2.53%
0x6a7f202E9D93A621A920ceB1F6707608cF4aa11D	14650	12432	-2217	-15.13%
0x274451e4611F6e55Bee7ef1e461d0c5Dd8152eBA	52898	50819	-2078	-3.92%
0xEc6e9E3fc69212510aa3f290dCB72070DD01fE19	29435	44820	15385	52.26%
0x8aD14c5f98d480A35d5716Adf7B296f8Ed6f5AB4	89158	80484	-8673	-9.72%
0x895c74080DD3672Ae30E92Af5cB7A1B1422fE866	73752	70025	-3726	-5.05%
0x15ec412Ba9670a69544009A80B8c10d9450f233a	11299	8871	-2427	-21.48%
0xE46387dB8B90D74b8a0d519E1B5D3070E8F00589	50254	46913	-3340	-6.64%
0x6C349a3787De27e2a85628291869968F6cc16ddD	9864	8832	-1031	-10.45%
0xc9da618A77839A0Cc4496104C20620cd65D05a64	74945	64685	-10259	-13.68%
0x1F7E0b237D2e5Fa8d54647727b3eBe24E28F6D97	33861	31074	-2786	-8.23%
0x9926abaFb48A1B1A34aA8c14Ca24C140f29e62c5	30253	25747	-4505	-14.89%
0xA6d68B32B83C4f91891fc767693270817F603B36	1611	1604	-6.3	-0.39%
0x41228e5dE79cD3cD0b7C09f8D9D2d4c193b8424B	36122	31157	-4964	-13.74%
0x7a2125c47014d57228FD7f4E90663729921fFFCa	72788	61446	-11341	-15.58%
0x27b4f9777098d1796EA361dc5448c598Ca71d997	57912	49727	-8184	-14.13%
0xE8Ff99b2D2cf3f2Cb1C86878e2e46D961B250CCc	10460	10348	-111	-1.07%
0x2505E965Ce868668617Ac7640c6C375F945a2905	24711	72453	47742	193.2%
0x85358ed0cFEeD598D1A7dCF23056890C02b0A354	76321	74619	-1701	-2.22%
0x871AA17AF26f7730003F128bBC872Bd0AD7817a8	56250	51257	-4992	-8.87%

Tabella 8: dati per i bot dal 67° a 99°: Paycoin iniziali e finali, variazione assoluta e percentuale.

Indirizzo bot	Fee pagate (PC)	% sui PC iniziali
0x5392927A750499B27C140ba843b2ca30F5F0E2a4	111	0.26%
0xe2Ea05a1FC8a522C78fA7A3561F455fb8e6Ee708	888	1.0%
0x7e354aA981B6dbE3C66037033152c86FA68518C3	43	0.06%
0x99d06632445AfAc088A7E6050A6747aa01f744d5	143	0.18%
0x012Ed6cC8A5F4E0A26defeADbFb7b365C2d55060	42	0.05%
0x0F27B686873b17BB8DE85e3F3268d2b402A2819f	137	0.16%
0xfBA6c71B68Ab867e03ECA385D65a60B385720FfC	3.3	0.09%
0x3FC1168d4EC8511d92D46A907E50509584b41e9f	52	0.07%
0xb71a10753da50d4Dc8e78B603342B7F5465D7415	69	0.17%
0x4F76743E6C975Bab7D46b8Aefc99802231F9FD08	140	0.17%
0x6C9BA7A6Ffeb5Ffa1bFBaC31325438812bE770a9	33	0.13%
0xE9C23E1f4dF8b934a218d2ac497ee28AE680f649	23	0.21%
0x7252B9276d057842970A882a1328dc08917006B4	66	0.13%
0xe01667456C2fa6A2dF68525C39a85A155B84B093	227	0.23%
0xb2Dc0ac6406193B546DEc16acFb08ecD13D08584	1.5	0.04%
0xaE4bF961ffB2b51870047D44Bac95Bd6e400A426	1.2	0.05%
0x4D09b13a42393f4cf2147666f1461EF68471866A	8.2	0.04%
0x5bD6C66b42Cd58583079a3552663Fb49a7A78A1D	97	0.17%
0xbC8511E3a7098CD394A368a04801c3390BE61bE4	82	0.16%
0x766dF54e7ccDec373410FEbc7Fcac14dC4a2bF3A	191	0.37%
0x563cFc69DE81627d26F82802317b753741c4B52b	62	0.18%
0x74BE597A72EF4e4Ff3313C05bFcaaA7f961bC09B	30	0.04%
0x384D9e3F1Fae476a79e3152784Db56B2a374c280	62	0.07%
0x225c651D54B4021793B03EE0A74d354343e6ca98	46	0.19%
0x5627b9874BeDC9dc27f92908E384171678c8FfCd	78	0.91%
0xB9F1c48A333c176634803aefb2c11450Bf11E5ef	374	0.63%
0xE067d75A81eB2Bc1b9C8Bbed919a370fE46c631B	78	0.19%
0xEdbD8723FcF67a4D675726a034c11C9A81E22a63	69	0.22%
0x228762d14e93A9bB5e9B4F69D3f4bd55657aa3B6	134	0.28%
0xcF313B3Ebc584a2596C9f1ff352cD6215FBc84f2	25	0.21%
0x158DBD55cc67C54E43459894C4d4f4E9F566D3E3	50	0.11%
0x1A6a254aFE9b9b65aEcd1c9EA04E7521da03186E	26	0.12%
0x1Af5F9152A833ff2d30585536EC6421A7Df2BF4d	34	0.09%

Tabella 9: dati per i primi 33 bot: fee totali pagate e percentuale sui Paycoin iniziali.

Indirizzo bot	Fee pagate (PC)	% sui PC iniziali
0x2EF92db880e619701c15177F710bC107720aBa11	123	0.12%
0x88e18973562d2F22E6138938035E0eB0f96578fC	32	0.13%
0xe08B1925201E5A5FA2BfAC6A2E5f348E4dba19B8	16	0.14%
0xe71D0C2059Ad76497D3697f24961f5E81d61F039	172	0.21%
0x7b3B037345cA2F878687fdA8D8f3A6580E436Bd3	123	0.15%
0x701D54b96d88f8077feEc2C15a5BeF7D1E6cb202	1.5	0.04%
0x6B3F9874b4b13Dac5e4d8182374B0aD20Cf0a5d2	4.1	0.04%
0xec23b31f616D96c95cdc2F32D9225dA47d695d1F	1.8	0.01%
0x48fCC9ccA03f0476455c3291b4Af71aD8E4bbd2e	134	0.17%
0x060fcfF0F88ae5D33367c8b4139d64E2277cC0d4	39	0.13%
0xeC557115C7A0e9347d56566043D9B9B847d25dec	17	0.06%
0x8B9540D8ea478CdEB736e1f5F82E566EfD1342c8	66	0.08%
0x33035ED633A3cED9005Ece48CF65f164B430199C	580	0.82%
0xfDf0b19f842f564D309a351E1eDC5250f06e7b3B	295	0.61%
0x380351dC5Ebd4aC5117cA7b8F2343b97B3C03e0b	147	0.15%
0x63B697a6D43C37d2B24f32a6303B57B5DD5D47ef	657	0.75%
0x45E2E2B28EfC9f3890F7411CBbF0F4fa5E84E066	440	0.63%
0xA73A8Ad1add220dfFcE68BACe1E89a6481E7fdCF	72	0.07%
0xd82bDeAc4dc8Ad2858aCB82eb03f2Dd949991d16	15	0.12%
0x6BF3dDa6FF3C67AC3b35C102fb68cBe8899059Be	287	0.53%
0x48F041F1b2408E9b0A762907626Ea056BC70fE9A	43	0.11%
0x2D242ACd72f1199177BAA71bC099DBa2BBe2ed3f	32	0.08%
0xEcFBe2844093e016717324429459E480213c29c9	10	0.05%
0x6789b513c7483c35232Bb084d5245E5aDDE58206	230	0.5%
0xcb5AE51F1F145626E49e54cEbFD8943692Aa8020	161	0.23%
0x0Dab9E319fb3756197E867b6014b107284Ef95E7	68	0.42%
0x117A3642e3407856eC5223Fc1AF22Ec9A4B85B2B	151	0.22%
0x472C53d0BBEC2efAEFcAFE1969BD1668a3161C9f	107	0.17%
0xad3d3011c58E47339795BdA8c9A478d71d6f75d2	160	0.17%
0x52ecfE54606b8a705afA046cFF74cf7FAD415a9D	39	0.22%
0xDd6AD0fb33Ffe17DBE2822409A9073a674e88926	101	0.1%
0xa2CA083d008d9A59E22eBa3B6f64714bf816c110	77	0.08%
0x1d2Cbbe57207053375F70Ef28E405f605dEf2051	232	0.26%

Tabella 10: dati per i bot dal 34° al 66°: fee totali pagate e percentuale sui Paycoin iniziali.

Indirizzo bot	Fee pagate (PC)	% sui PC iniziali
0xC280370BCcDcf9D918767ccC158c8dF53dB2D2e7	59	0.08%
0x6B943c96FeF8845A2Fff7a9aBCaC82db0a6F0c9D	51	0.05%
0xdB6485c575781bBeF3F79EDFC85D246DaE2BA8Ba	17	0.03%
0xF71C4A52a5ae9dd1fBd30670c6310c423E7f78F5	35	0.18%
0x048421bFf43B016439B35684e69C54dCC581526D	120	0.2%
0x3c83f996b9A898aff6A41Ff8b03AE05d2DF08871	156	0.2%
0xD44e43CaE6e51D64a48e781756D1F05eeF0e3b2F	49	0.08%
0xdb8b0217c5089784eb49D84763f8bc82365e8726	3.3	0.05%
0x2845867f16C77771dCC61B855E4312CcAAc64878	172	0.39%
0xee6bd0A5f5287eC909F30ca5180f35da00632440	33	0.08%
0x4f209Ee52FcB45C1B47302a4299fe30E9B9D8aDC	229	0.28%
0x07DA069d0902649Df096e53185c3626e9469Aaf6	103	0.24%
0xB89b7Cc588D998602cC283C67a4b9e8F1F4859db	59	0.09%
0x32eAdeB7A1c8310fa31b417ea8E862eBa5d6475C	16	0.06%
0x6a7f202E9D93A621A920ceB1F6707608cF4aa11D	20	0.14%
0x274451e4611F6e55Bee7ef1e461d0c5Dd8152eBA	49	0.09%
0xEc6e9E3fc69212510aa3f290dCB72070DD01fE19	196	0.66%
0x8aD14c5f98d480A35d5716Adf7B296f8Ed6f5AB4	25	0.02%
0x895c74080DD3672Ae30E92Af5cB7A1B1422fE866	21	0.02%
0x15ec412Ba9670a69544009A80B8c10d9450f233a	18	0.16%
0xE46387dB8B90D74b8a0d519E1B5D3070E8F00589	75	0.15%
0x6C349a3787De27e2a85628291869968F6cc16ddD	10	0.1%
0xc9da618A77839A0Cc4496104C20620cd65D05a64	57	0.07%
0x1F7E0b237D2e5Fa8d54647727b3eBe24E28F6D97	8.3	0.02%
0x9926abaFb48A1B1A34aA8c14Ca24C140f29e62c5	46	0.15%
0xA6d68B32B83C4f91891fc767693270817F603B36	0.7	0.04%
0x41228e5dE79cD3cD0b7C09f8D9D2d4c193b8424B	43	0.11%
0x7a2125c47014d57228FD7f4E90663729921fFFCa	96	0.13%
0x27b4f9777098d1796EA361dc5448c598Ca71d997	191	0.33%
0xE8Ff99b2D2cf3f2Cb1C86878e2e46D961B250CCc	1.2	0.01%
0x2505E965Ce868668617Ac7640c6C375F945a2905	355	1.44%
0x85358ed0cFEeD598D1A7dCF23056890C02b0A354	33	0.04%
0x871AA17AF26f7730003F128bBC872Bd0AD7817a8	81	0.14%

Tabella 11: dati per i bot dal 67° al 99°: fee totali pagate e percentuale sui Paycoin iniziali.