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

CONTENUTI DELLA PRESENTAZIONE

- Descrizione della tecnologia Blockchain
- Introduzione sui progetti di exchange decentralizzati
- Introduzione sul concetto di market making automatico
- Descrizione della piattaforma sviluppata
- Analisi dell'utilizzo della piattaforma

L'obiettivo del progetto è la creazione di un exchange decentralizzato, utilizzato per una gara di trading.

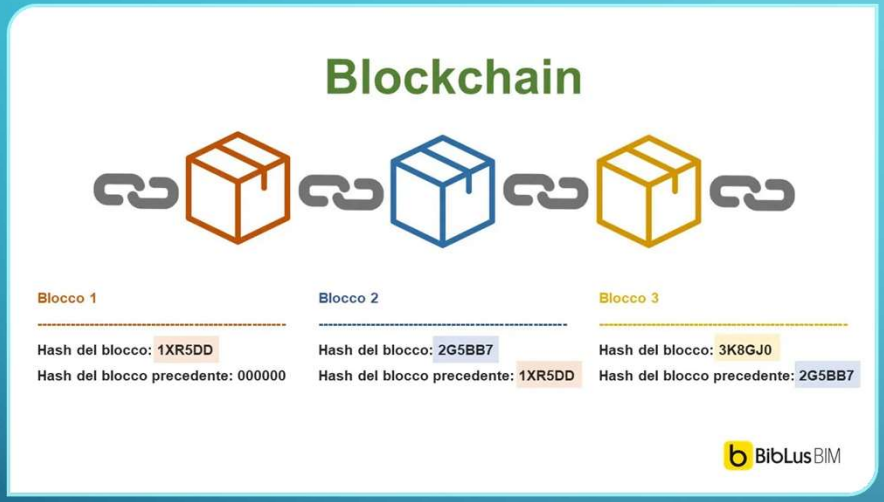
LA BLOCKCHAIN: COS'È E COME FUNZIONA

- Una *blockchain* è un registro digitale aperto e distribuito, in grado di memorizzare insiemi di dati, detti transazioni, in modo sicuro, verificabile e permanente.
- I dati sono salvati in blocchi, che sono collegati uno all'altro mediante l'utilizzo di tecniche crittografiche, rendendo di fatto irreversibili le transazioni.

LA BLOCKCHAIN: LE CARATTERISTICHE

- **Decentralizzazione:** le operazioni non sono gestite da nessun ente centrale/intermediario.
- **Trasparenza:** il contenuto del registro è visibile a tutti.
- **Immutabilità:** una volta registrati, i dati non possono essere modificati, se non con il consenso dell'intera rete.

LA STRUTTURA DEI BLOCCHI



- Le transazioni sono raggruppate all'interno dei blocchi della blockchain. Ogni blocco contiene l'hash crittografico del blocco precedente, un timestamp, e dei dati di transazione.

VALIDAZIONE DELLE TRANSAZIONI

- Un indirizzo della blockchain possiede una chiave pubblica, visibile a tutti, e una chiave privata, che solo il proprietario conosce.
- La validazione delle richiesta di transazione avviene con tecniche crittografiche effettuate da utenti, detti *miners*.
- Queste tecniche richiedono una certa potenza computazionale (rischio della decentralizzazione dei nodi).

LA BLOCKCHAIN DI BITCOIN

È la prima blockchain inventata. Viene creata nel 2008 da Satoshi Nakamoto (pseudonimo), contestualmente alla crypto Bitcoin.

Permette lo scambio peer-to-peer di valuta. Il valore del bitcoin è determinato unicamente dalla leva di domanda e offerta.

La validazione delle transazioni avviene attraverso tecniche crittografiche.

LA BLOCKCHAIN DI ETHEREUM

- È una blockchain finalizzata alla creazione e pubblicazione di contratti intelligenti (*smart contracts*), programmi che possono girare sulla rete.
- Ad essa è associata una cryptovaluta di scambio, detta Ether.
- Gli smart contracts pagano la potenza computazionale della rete attraverso commissioni in Ether.
- Ad ogni contratto è associato un indirizzo, come per ogni utente.

GLI EXCHANGE DECENTRALIZZATI (DEX)

- Sono delle piattaforme che permettono lo scambio di crypto senza l'intermediazione di un ente centrale.
- L'utente può attingere alle proprie valute direttamente dal proprio wallet (protetto da una chiave privata).
- Lavorano *on-chain*.

VANTAGGI E SVANTAGGI DELLE DEX

VANTAGGI

- L'utente ha pieno possesso dei suoi fondi
- Non è necessaria la conferma dell'identità
- È possibile scambiare ogni tipo di crypto

SVANTAGGI

- È poco user-friendly
- Non è garantita la possibilità di scambiare token
- Se l'utente perde la chiave privata del wallet, perde definitivamente le crypto
- Commissioni più alte

RISCHI PRINCIPALI DEI DEX

I rischi principali derivano dalla natura aperta dei DEX e dalla mancata regolamentazione:

- La mancanza di un controllo favorisce la creazione di token truffaldini
- Gli utenti possono sfruttare a proprio piacimento bug negli smart contracts

Un altro fattore di rischio è rappresentato dalla lentezza della rete e dal fatto che le transazioni non sono istantanee.

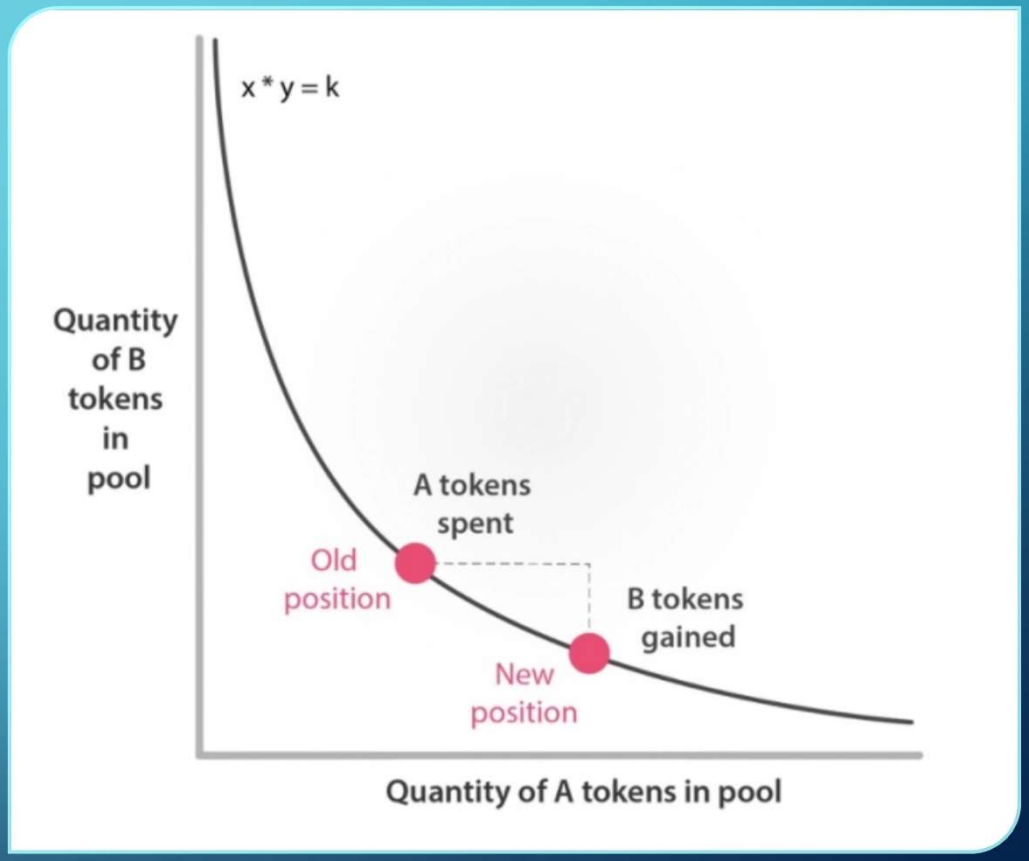
I MARKET MAKING AUTOMATICI (AMM)

- Sono un tipo di exchange decentralizzati che definiscono in automatico il prezzo tra due quantità.
- Hanno immediata disponibilità di compravendita.
- Si basano sul concetto di pool di liquidità: 'contenitori' di una coppia token acquistabili e vendibili.
- Esistono diversi tipi di AMM, in base all'algoritmo di calcolo del prezzo.

MARKET MAKER A PRODOTTO COSTANTE

- Il prodotto delle due quantità nella pool deve rimanere costante
- Alla diminuzione di una, corrisponde un definito aumento dell'altra

$$x \cdot y = k$$



ARCHITETTURA DEL SISTEMA IMPLEMENTATO

SMART CONTRACTS

- Token e Paycoin
- Pool
- Challenge

BOT E PYTHON

- Creazione di bot
- Scripts per lanciare funzioni
- Sistema di monitoraggio

GLI SMART CONTRACTS

Sono programmi (da noi scritti in linguaggio Solidity) che girano sull'EVM (Ethereum Virtual Machine). Hanno la seguente struttura:

- Costruttore: inizializza certe variabili nel momento della pubblicazione
- Funzioni: possono essere eseguite mentre il contratto è in rete
- Modificatori: contengono delle condizioni da verificare per la chiamata di una funzione
- Eventi: servono per salvare nella blockchain i valori di alcuni parametri

TOKEN - PAYCOIN

- I Paycoin sono l'equivalente della moneta pubblica.
- I Token sono la moneta di proprietà del loro creatore.
- Attraverso le pool, contenenti Token e Paycoin, si possono comprare e vendere i Token.
- Queste monete sono create con degli smart contracts che seguono un protocollo, detto ERC-20.

GLI SMART CONTRACTS DI TOKEN E PAYCOIN

PARAMETRI INIZIALI:

- Nome
- Simbolo
- Decimali (tipicamente 18)
- Importo iniziale

FUNZIONI PRINCIPALI:

- *minting*: creazione di token
- *transfer*: trasferimento
- *transferFrom*: trasferimento da parte di terzi
- *approve*: approvazione del trasferimento da parte di terzi

POOL

Sono il cuore dell'exchange, contengono Token e Paycoin e sono sviluppate con la formula del prodotto costante. Lavorano con i contratti di Token e Paycoin.

Tre tipi di pool nella gara, in base alla liquidità iniziale:

- Pool con 100 Token e 100000 Paycoin
- Pool con 10000 Token e 100000 Paycoin
- Pool con 10000000 Token e 100000 Paycoin

LO SMART CONTRACT DELLA POOL

- *mint-liquidity*: inserimento della liquidità iniziale nella pool
- *buy*: acquisto di Token nella pool (k costante, cambia il prezzo)
- *sell*: vendita di Token nella pool (k costante, cambia il prezzo)
- *mint-stake*: aggiunta di liquidità nella pool (prezzo costante, cambia k)
- *burn-stake*: rimozione di liquidità nella pool (prezzo costante, cambia k)
- *day-mint*: minting giornaliero di Token nel wallet dell'owner

CHALLENGE

Sono state implementate delle sfide attraverso un ulteriore smart contract.

Un utente può sfidare uno o due partecipanti lanciando una challenge, vince chi richiama la challenge per primo dopo 20 secondi. I premi sono in Paycoin.

- Challenge 1v1: 1000 Paycoin per chi avvia, 10000 per chi vince
- Challenge 1v2: 2000 Paycoin per chi avvia, 50000 per chi vince

LO SMART CONTRACT DELLE CHALLENGE

Lo smart contract delle challenge contiene le seguenti funzioni:

- Lancio di una challenge singola
- Lancio di una challenge doppia
- Chiamata di una challenge singola
- Chiamata di una challenge doppia

Lo smart contract chiama lo smart contract Paycoin per trasferire i premi.

SCRIPTS IN PYTHON

Il progetto prevede l'implementazione di alcuni scripts in Python per quattro funzioni:

- Creazione di un sistema di bot che svolgano operazioni di compravendita casuali, per generare del rumore nel mercato.
- Funzioni per facilitare l'utilizzo degli smart contract.
- Sistema di monitoraggio per salvare periodicamente i parametri della gara (prezzo dei Token, liquidità delle Pool, bilanci dei partecipanti…)
- Sistema di monitoraggio delle challenge che avverte gli sfidanti tramite un bot di Telegram.

SCRIPT DEI BOT

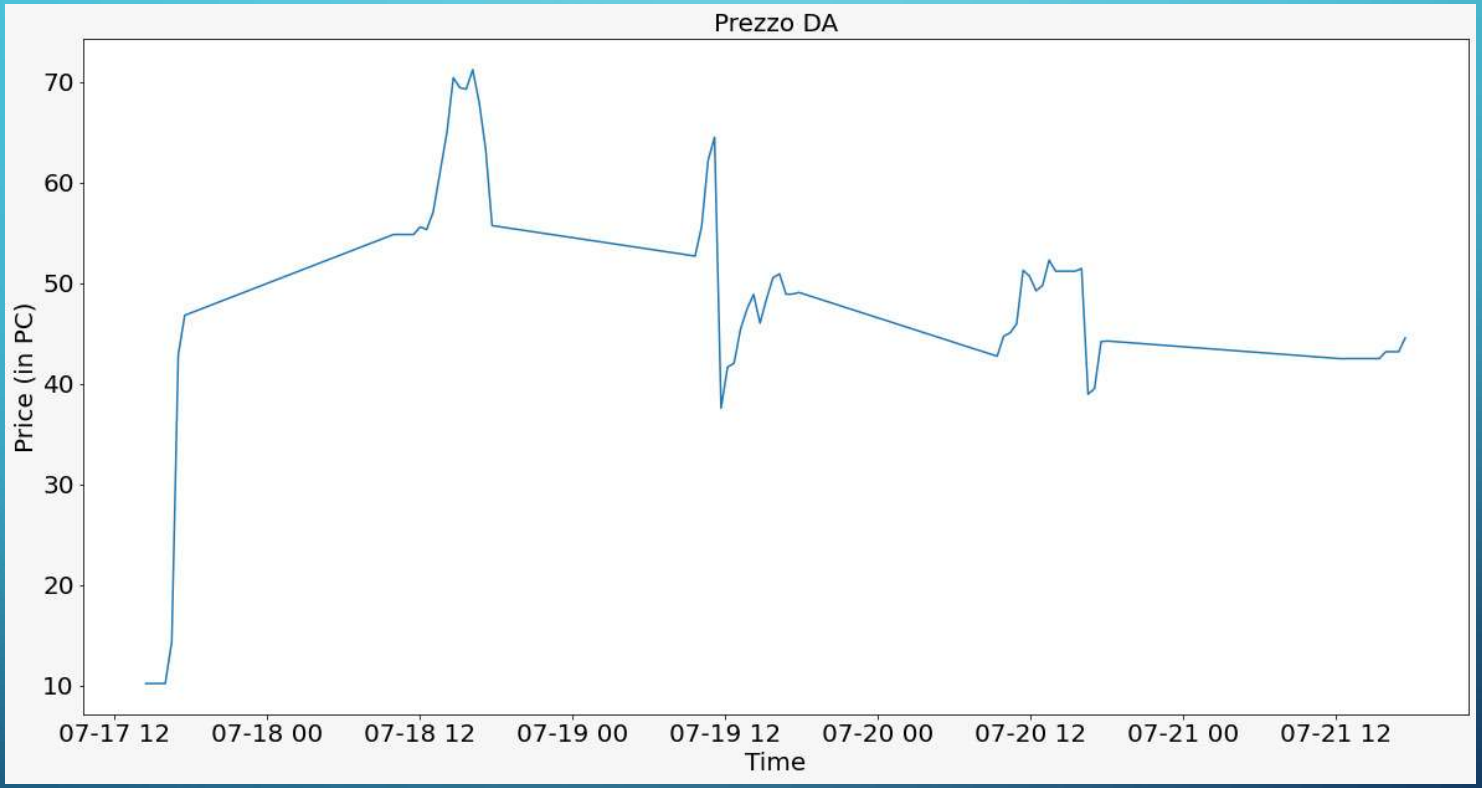
- Sono stati generati 100 account, ognuno con chiave pubblica e privata, che svolgevano le funzioni dei bot.
- Ad ognuno di questi indirizzi sono stati trasferiti degli Ether e un numero casuale di Paycoin compreso tra 1000 e 100000.
- I bot hanno lavorato grazie ad uno script con un ciclo infinito che ogni minuto eseguiva casualmente operazioni di *buy* e *sell* nelle pool.
- I bot sono stati gestisti da un quarto account (admin).

ANALISI DELL'ANDAMENTO DELLA GARA

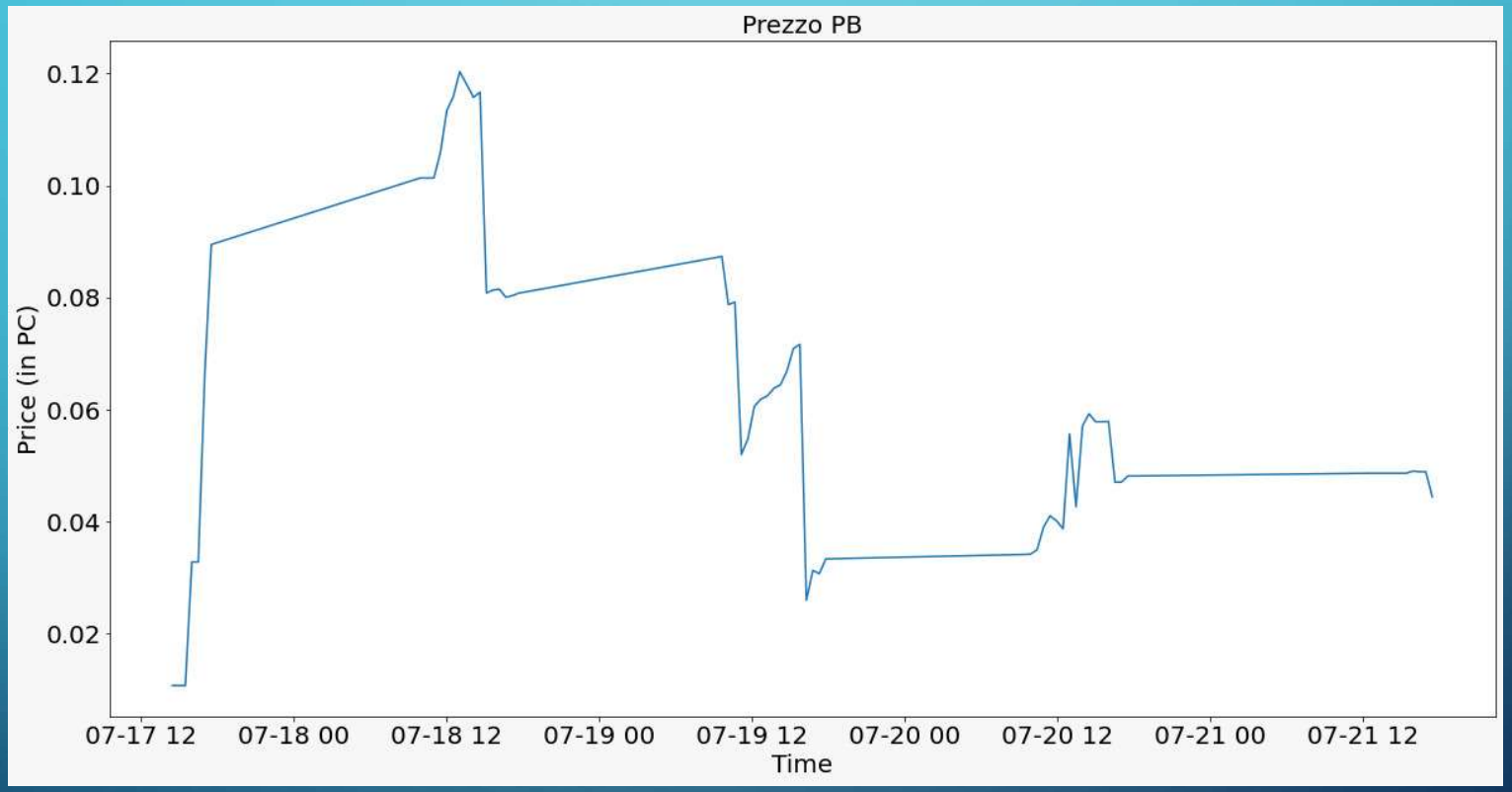
I tre partecipanti sono Daniele, Paolo e Giovanni. Ad ognuno è affidata la gestione di un Token e di una pool:

- Daniele: Token DA, prezzo iniziale di 10 PC/DA
- Paolo: Token PB, prezzo iniziale di 0.01 PC/PB
- Giovanni: Token GR, prezzo iniziale di 1000 PC/GR

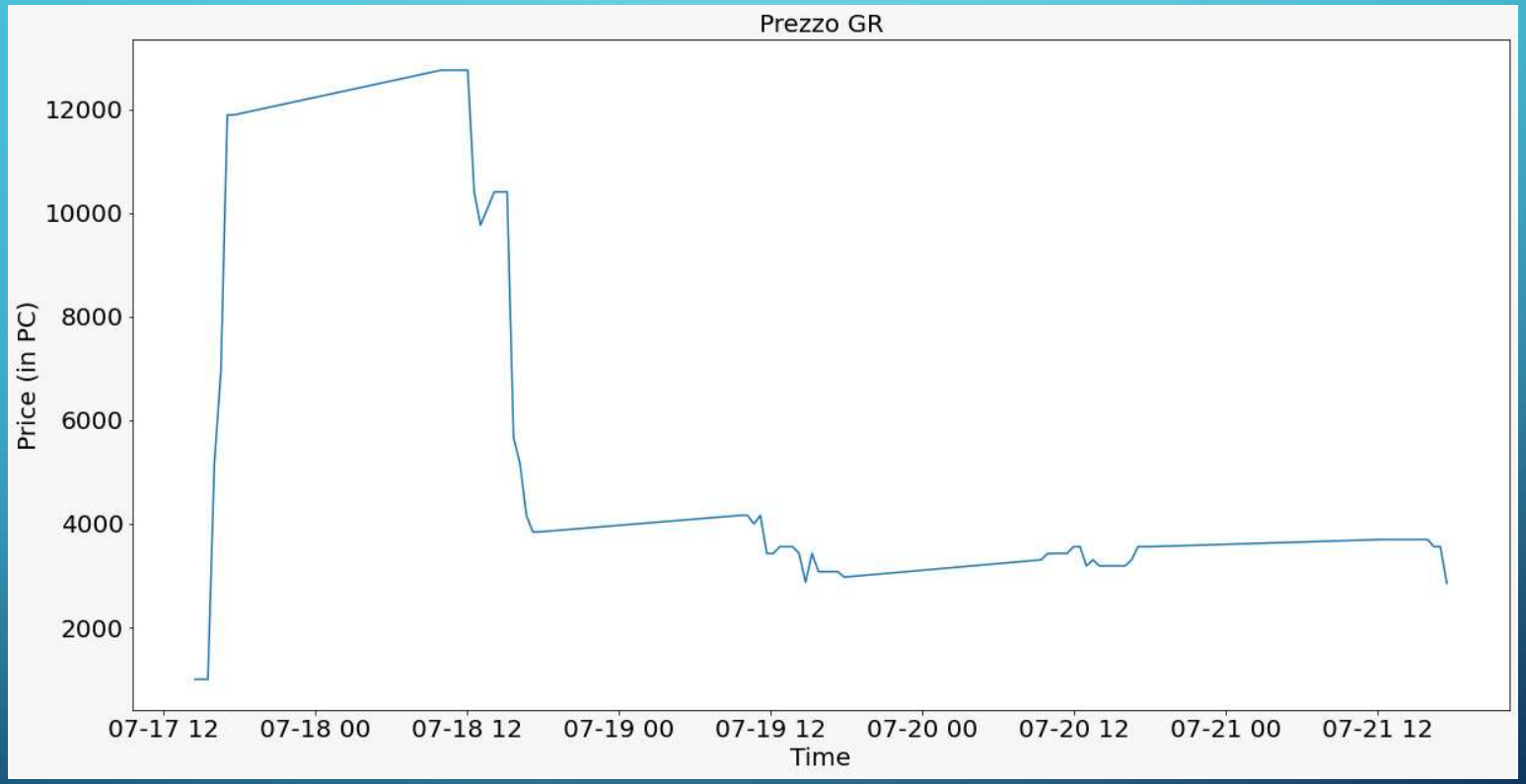
ANDAMENTO DEL PREZZO DEL TOKEN DA



ANDAMENTO DEL PREZZO DEL TOKEN PB



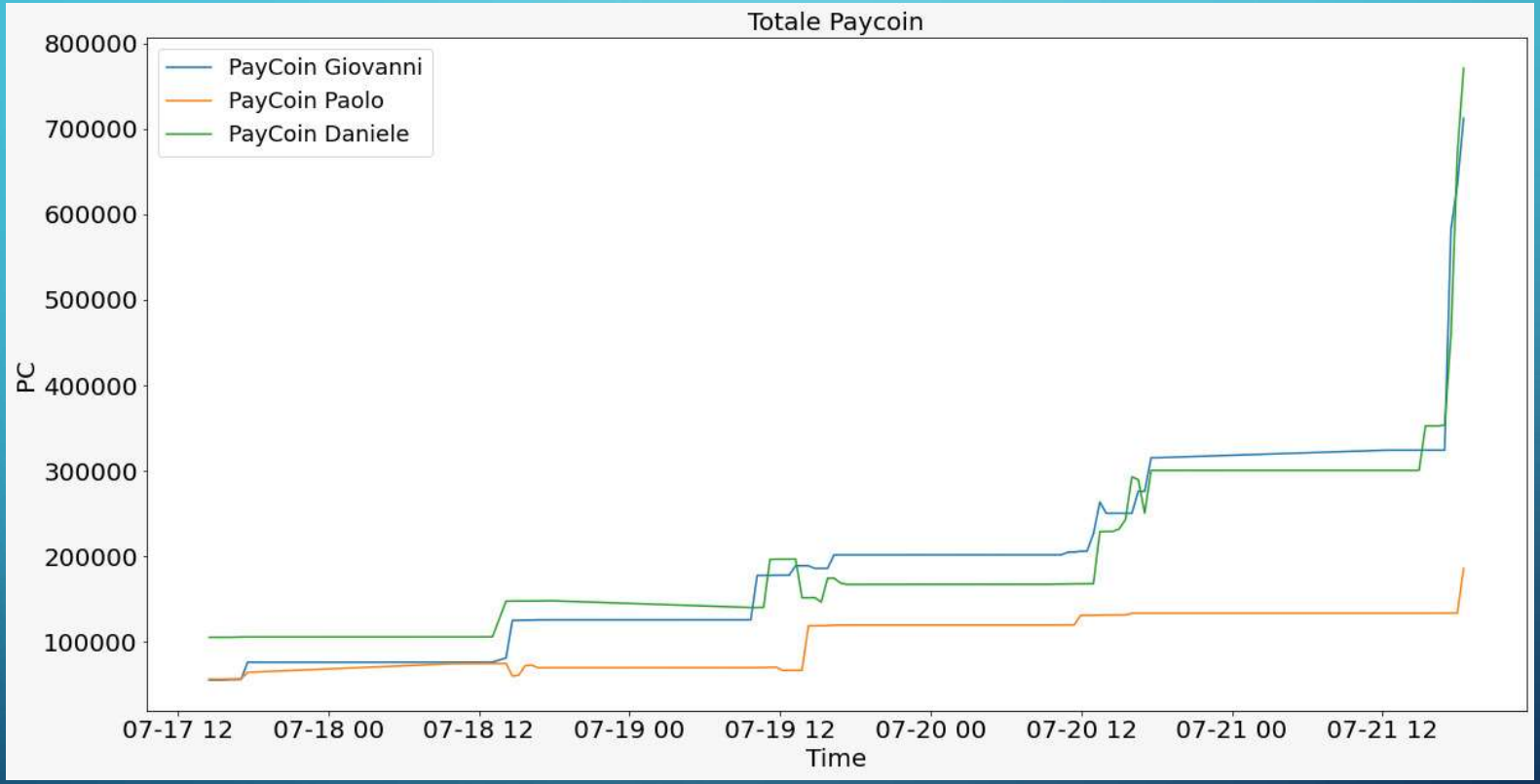
ANDAMENTO DEL PREZZO DEL TOKEN GR



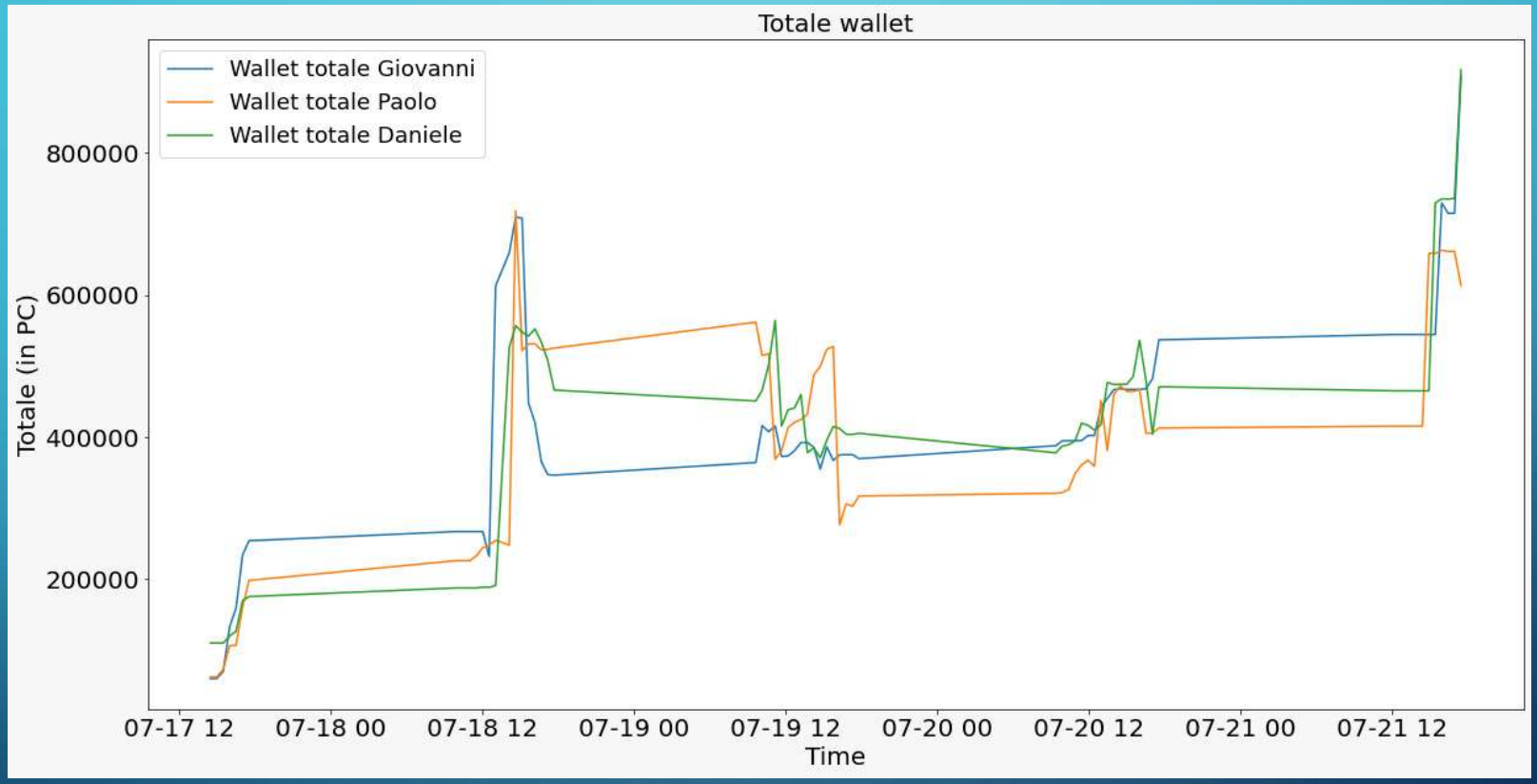
COMMENTI SULL'ANDAMENTO DEL PREZZO

- Tutti e tre i grafici presentano una forte crescita iniziale: questo è dovuto ad un malfunzionamento dei bot, che a inizio gara hanno comprato grosse quantità di Token senza rivenderli.
- Dopo aver risolto il bug, i prezzi si sono abbassati e le successive oscillazioni sono dovute ad operazioni di compravendita.
- Il prezzo con più oscillazioni è stato quello del Token PB, quello con meno oscillazioni è stato quello del Token GR.

ANDAMENTO DEL TOTALE DI PAYCOIN NEI WALLET



ANDAMENTO DEL VALORE TOTALE NEI WALLET



GUADAGNO/PERDITA IN PAYCOIN

- L'andamento dei PC nei wallet è in crescita per tutti e tre gli utenti.
- Le salite più marcate corrispondono a vittorie nelle challenge, mentre le oscillazioni meno ampie rappresentano operazioni di trading.
- Il grafico del valore totale del wallet rappresenta solo ricchezza *virtuale*, la ricchezza reale è rappresentata dai Paycoin.

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%

RISULTATI DELLE CHALLENGE

La maggior parte dei guadagni derivano dalle challenge.

Non sono state esaurite tutte le challenge a disposizione.

Sono state lanciate molte challenge nell'ultima mezz'ora.

Daniele e Paolo hanno perso circa 15000 PC in trading, mentre Giovanni ne ha guadagnati 40000.

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

SWAP EFFETTUATI

Il numero di swap non cambia particolarmente tra le tre pool.

Nelle pool di Daniele e Giovanni la differenza tra i *buy* e i *sell* è di ordine 10.

Nell pool di Paolo sono stati fatti 29 *buy* in più rispetto ai *sell*.

Pool	n° *buy*	n° *sell*
Daniele	242	252
Paolo	241	212
Giovanni	212	220

FEE PAGATE

- Le fee pagate risultano essere sotto l'1% dei Paycoin iniziali.
- Le fee spese sono indice dell'attività dell'utente: Giovanni è stato l'utente più attivo, seguito da Daniele e Paolo.
- I bot, in totale, hanno una percentuale di fee pagate sui PC iniziali paragonabile a quella di Paolo.

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%

PROBLEMI E ANOMALIE RISCONTRATI

PROBLEMA

A inizio gara i bot compravano troppi token, creando variazioni nei prezzi tutt'altro che trascurabili e quindi non considerabili rumore.

SOLUZIONE

Modifica dello script dei bot, in particolare della modalità di estrazione dei valori di Token che questi vendevano e compravano.

PROBLEMI E ANOMALIE RISCONTRATI

PROBLEMA

Bug nei contratti delle pool e negli scripts, per quanto riguardava le funzioni di *mint-stake* e *day-mint*.

SOLUZIONE

- Modifica dello script che lanciava la funzione di *mint-stake*.
- Modifica del contratto (non possibile durante la gara) della pool per correggere l'errore nella funzione *day-mint*.

PROBLEMI E ANOMALIE RISCONTRATI

PROBLEMA

Impossibilità di effettuare swap tra il proprio Token e quelli altrui, in quanto per questa operazione venivano direttamente chiamate le pool dei due Token.

SOLUZIONE

Creazione di un terzo contratto che poteva fungere da tramite per le operazioni di swap, interagendo con le pool.

PROBLEMI E ANOMALIE RISCONTRATI

PROBLEMA

Negli ultimi due giorni della gara la rete è diventata più lenta e le transazioni richiedevano molto tempo per essere confermate.

SOLUZIONE

Aumentare il limite di gas pagato per le transazioni, in modo che queste avessero maggiore priorità.


GRAZIE PER L'ATTENZIONE!