

Università degli Studi di Napoli “Parthenope” www.uniparthenope.it

Dipartimento di Scienze e Tecnologie

Centro Direzionale Isola C4

80143 Napoli - Italy

**Reti di Calcolatori e Laboratorio di Reti di Calcolatori**

A.A. 2018-2019

**Progetto** **BlockExplorer**

**Studenti:**

|  |  |  |
| --- | --- | --- |
| COGNOME | NOME | MATRICOLA |
| Bevilacqua | Vincenzo | 0124001490 |
| Di Marino | Antonio | 0124001344 |

**Docente:** Alessio Ferone

INDICE

[Descrizione del progetto 3](#_Toc3843705)

[Descrizione e schemi dell’architettura 4](#_Toc3843706)

[Schema della rete 4](#_Toc3843707)

[Descrizione della rete 4](#_Toc3843708)

[Protocollo di livello trasporto 5](#_Toc3843709)

[Descrizione e schemi del protocollo applicazione 6](#_Toc3843710)

[Schema generale 6](#_Toc3843711)

[Descrizione schema generale 7](#_Toc3843712)

[Schema Generazione Blocchi 8](#_Toc3843713)

[Descriziome Generazione Blocchi 8](#_Toc3843714)

[Schema Trasferimento Blocchi 10](#_Toc3843715)

[Descrizione Trasferimento Blocchi 10](#_Toc3843716)

# **Descrizione del progetto**

Il progetto si pone l’obiettivo di analizzare una *blockchain*, essa è una sequenza di blocchi in cui ogni blocco contiene una transazione.  
La rete si compone di tre entità fondamentali, un *NodoN*, un *BlockServer* e un *BlockClient*.

Un *NodoN* è un ` entità che simula una blockchain e ne salva la copia su di un file, il *BlockServer*  ha il compito di connettersi con il *NodoN* per ricevere una copia della blockchain e fornire informazioni su di essa ad uno o più *BlockClient* , il *BlockClient* a sua volta si connette al *BlockServer* per poter analizzare le transazioni contenute nella blockchain.

# **Descrizione e schemi dell’architettura**

## Schema della rete

## Descrizione della rete

La rete si compone di un *NodoN* che genera blocchi casuali in una blockchain per poi salvarli in un suo file locale “blocchi\_nodon.txt”.  
In una visione più ampia della rete il *NodoN* si collega ad una rete di peer dove la funzione principale è quella di scambiarsi i blocchi di una blockchain, in questo progetto invece si presuppone che tutto ciò già avvenga, per cui il trasferimento dei blocchi viene simulato generando i blocchi casualmente, quindi il *NodoN* verrà utilizzato solo come **server**. La finalità di questo progetto consiste nell’analisi dei blocchi e per tal fine si necessita di un solo *NodoN*.

Il *BlockServer* è l’entità che ha una doppia funzionalità, esso si occupa di reperire i blocchi connettendosi al *NodoN* e di salvarli in un proprio file locale “blocchi\_blockserver.txt”, inoltre si occupa di fornire ad n *BlockClient* dei servizi di analisi della blockchain.

Il *BlockClient* rappresenta un generico client che vuole reperire informazioni riguardanti i blocchi della blockchain, esso si connette al *BlockServer* per interrogare la blockchain. In particolare, i *BlockClient* possono richiedere di:

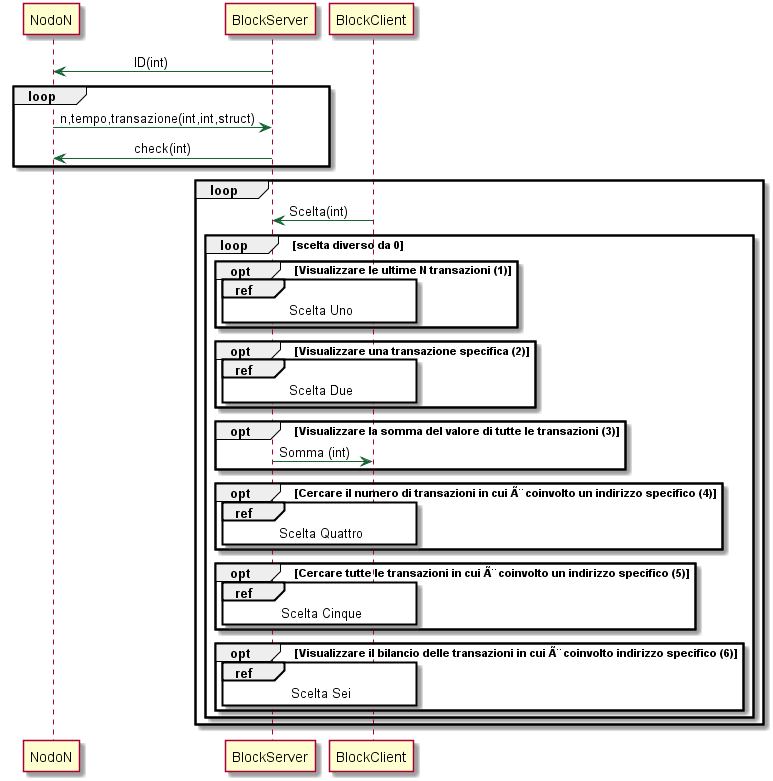
* Visualizzare le ultime n transazioni.
* Visualizzare i dati di una specifica transazione
* Visualizzare la somma dei valori di tutta la blockchain
* Visualizzare il numero di transazioni in cui è coinvolto un indirizzo specifico.
* Visualizzare i dati di tutte le transazioni in cui è coinvolto un indirizzo specifico.
* Visualizzare il bilancio delle transazioni in cui è coinvolto un indirizzo specifico.

## Protocollo di livello trasporto

Nel livello trasporto del TCP/IP si è scelto di utilizzare il protocollo **TCP** invece dell’UDP, dato che bisogna assicurare che i blocchi vengano correttamente trasferiti dal NodoN al BlockServer con un preciso ordine, bisogna considerare anche l’importanza delle transazioni che nella realtà dei fatti contengono denaro ed esse non possono essere perse, e infine dato che il TCP mantiene lo stato della connessione si possono monitorare e gestire ipotetiche cadute di connessione.

# **Descrizione e schemi del protocollo applicazione**

## Schema generale



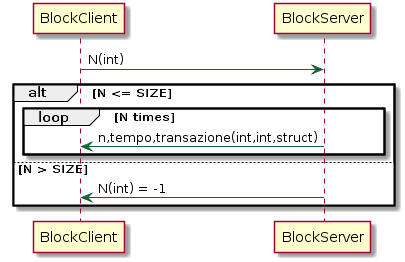
### Descrizione schema generale

Questo schema raffigura come a livello applicazione si svolgono le comunicazioni tra le entità in gioco. Il BlockServer invierà un intero al NodoN per comunicargli l’ultimo indice della blockchain che lui stesso possiede in modo tale che il NodoN gli invierà i restanti blocchi della blockchain (in loop), i blocchi vengono inviati sottoforma di struttura che contiene un identificativo numerico del blocco **n**, un **tempo** randomico e una sottostruttura **transazione** che a suo interno contiene come campi **IP**:**PORTA** Mittente, **IP**:**Porta** Destinatario , il **credito** da trasferire e **l’identificativo** della transazione. Il BlockServer invierà un intero (1) al NodoN ogni qualvolta riceve un blocco, questo intero avrà la funzione di check, cioè verrà usato per valutare la stabilità della connessione.

Per quanto riguarda la comunicazione client-server tra BlockClient e BlockServer, le richieste e le risposte avvengono diversamente in base al servizio richiesto dal BlockClient.

Il BlockClient invierà in tutti i casi un intero al BlockServer che corrisponderà al servizio scelto, di seguito poi verranno mostrati i protocolli di comunicazione tra BlockClient e BlockServer in base alla scelta effettuata.

## Schema Scelta Uno



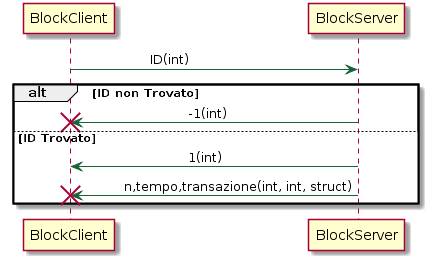
### Descrizione scelta uno

Per quanto riguarda il protocollo applicazione per l’analisi della blockchain , nel caso in cui il BlockClient richieda di visualizzare le ultime N transazioni (Scelta = 1 nello schema [pagina|6] ), allora le comunicazioni tra le due controparti avverranno come indicato nello schema sovrastante.

Il BlockClient richiede al BlockServer di inviargli gli ultimi N blocchi.

Se il BlockServer in quell’istante è in possesso dei blocchi richiesti, allora per N volte invierà i blocchi al BlockClient, altrimenti invierà al BlockClient un interno negativo (-1) che sta ad indicare che i blocchi richiesti in quell’istante non sono presenti nella blockchain.

# Schema Scelta Due

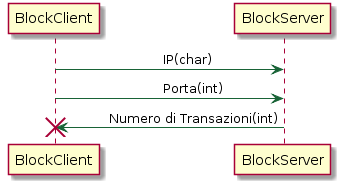


## Descrizione scelta due

Il BlockClient quando vuole visualizzare una specifica transazione, richiederà al BlockServer il blocco con uno specifico ID.

A sua volta il BlockServer andrà a controllare se il blocco con l’ID richiesto del BlockClient esiste nella sua blockchain in quel determinato istante, se non è presente viene inviato -1 , altrimenti viene inviato 1 per indicare che il blocco esiste, dopodichè viene inviato il blocco richiesto.

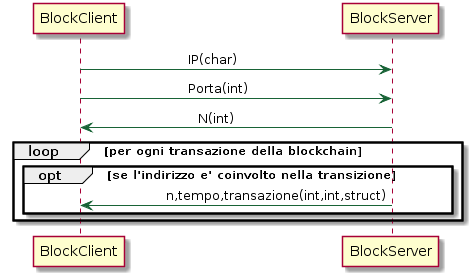
## Schema Scelta quattro



### Descrizione scelta quattro

Nel caso in cui il BlockClient richieda di conoscere il numero di transazioni in cui è coinvolto un determinato indirizzo (IP:Porta), il BlockServer gli invierà quante volte in quell’istante, l’indirizzo desiderato è presente nelle transazioni, nel caso in cui l’indirizzo non compare in nessun blocco, allora il Numero di Transazioni da inviare al BlockClient sarà pari a 0.

## Schema Scelta Cinque



### Descrizione scelta cinque

Nel caso in cui il BlockClient richieda di conoscere tutti i dati dei blocchi in cui è coinvolto un determinato indirizzo (IP:Porta), il BlockServer cercherà in quante transazioni è coinvolto quel determinato indirizzo in quell’istante, dopodiché invierà al BlockClient il numero di volte in cui l’indirizzo è presente, per far si che sia il BlockClient che il BlockServer comunichino lo stesso numero di volte per trasferirsi i blocchi, infine per ogni blocco il BlockServer invierà al BlockClient i loro dati.

## Schema Scelta Sei

## 

## Descrizione scelta sei

Nel caso in cui il BlockClient richieda di conoscere il bilancio in cui è coinvolto un determinato indirizzo (IP:Porta), il BlockServer calcolerà il bilancio in base alla presenza dell’indirizzo nelle transazioni come mittente o destinatario, dopodiché se il BlockServer ha trovato delle transazioni, invierà al BlockClient quante volte ha trovato l’indirizzo e poi gli invia il bilancio, altrimenti invierà al BlockClient che l’indirizzo è stato trovato 0 volte.

# **Dettagli implementativi del client**

Prima di analizzare le scelte implementative effettuate con il linguaggio di programmazione C, è di fondamentale importanza introdurre la struttura dei blocchi e il loro contenuto:

1. **struct** Blocco
2. {
3. **int** n;
4. **int** tempo;
5. **struct** Transazione ts;
6. **struct** Blocco \*next;
7. } ;

n: Rappresenta l’identificativo progressivo dei blocchi, che in questo progetto parte da 0 con il blocco **genesi**.

tempo: Rappresenta un tempo randomico compreso tra 5 e 15 secondi che il NodoN deve attendere prima di inserire un nuovo blocco nella blockchain.

next: Rappresenta un puntatore al successivo blocco, considerando che la blockchain viene rappresentata come una lista.

La transazione ts è a sua volta una struttura così definita:

1. **struct** Transazione
2. {
3. **char** ipMittente[16];
4. **int** portaMittente;
5. **int** credito;
6. **char** ipDestinatario[16];
7. **int** portaDestinatario;
8. **int** numRandom;

};

L’interfaccia client del BlockServer ha lo scopo di richiedere e ricevere i blocchi dal NodoN il cui protocollo applicazione è stato introdotto a [pagina 6], la scelta implementativa che è stata adoperata in questo progetto si avvale di un thread “**ottieniNodi**” creato dal BlockServer.

Si è scelto di utilizzare i thread per garantire la concorrenza sulle varie azioni che può effettuare il BlockServer, un’alternativa potrebbe essere l’implementazione di un I/O Multiplexing con l’ausilio della select. La differenza sostanziale sta nel fatto che con il thread abbiamo piena autonomia delle azioni ed esse sono indipendenti l’una dall’altra, eccezion fatta per le sincronizzazioni tra i thread su alcune sezioni critiche, mentre con l’I/O Multiplexing si delega al kernel il monitoraggio dei canali di comunicazione pronti ad essere utilizzati, dopodiché se il kernel sblocca il processo dalla select, bisognerebbe controllare sequenzialmente quale di questi canali risulta essere disponibile.

La funzione di **ottieniNodi** è quella di connettersi al NodoN, inviargli l’identificativo dell’ultimo blocco della sua blockchain, poiché si prevede che il NodoN gli risponde sempre inviandogli il successivo blocco utile. In seguito, viene illustrato la porzione di codice che riguarda la comunicazione del thread BlockServer con il BlockClient.

1. printf("BLOCKSERVER: Chiedo al nodon i blocchi dall'indice: %d\n", numBl+1);
2. FullWrite(socket, &numBl, **sizeof**(**int**));
4. **while**( FullRead(socket, &t, **sizeof**(**struct** temp)) != -1 )
5. {
6. **if** (t.n == size+1)
7. {
8. pthread\_mutex\_lock(&mutex);
9. inserimentoCoda(t, genesi);
10. size++;
11. write(file, &t, **sizeof**(**struct** temp));
12. printf("THREAD BLOCKSERVER: Blocco ricevuto ed inserito: %d.\n\n", t.n);
13. pthread\_mutex\_unlock(&mutex);
15. printf("n = %d\ntempo = %d\nIp Destinatario: %s\t Porta: %d\n", t.n,t.tempo, t.ts.ipDestinatario, t.ts.portaDestinatario);
16. printf("Ip Mittente: %s\t Porta Mittente: %d\nCredito: %d\nNumero Randomico: %d\n\n\n\n", t.ts.ipMittente, t.ts.portaMittente, t.ts.credito, t.ts.numRandom);
17. }
19. FullWrite(socket, &check, **sizeof**(**int**));
20. }

In questa porzione di codice si è scelto di creare una sezione critica, a cui si accede con un mutex, questa implementazione è stata utilizzata per soddisfare la legge di Bernstein sulla variabile globale size (che viene modificata da questo thread e letta da un altro thread), per garantire che il blocco venga considerato appartenente alla blockchain solo quando esso viene scritto anche in modo permanente sul file locale, e infine in modo tale da garantire che se in futuro altri thread (**gestoreClient**) effettuassero delle analisi sulla blockchain in mutua esclusione con questo mutex, allora nel frattempo questo thread **ottieniNodi** dovrà attendere che l’analisi venga completata prima di aggiornare la blockchain.

Una particolare nota sulla gestione di questo thread **ottieniNodi** riguarda l’utilizzo dei segnali e del gestore dei segnali, nel caso in cui il NodoN si disconnette da questa comunicazione. In particolar modo, quando il thread **ottieniNodi** si rende conto che la connessione è stata terminata dal NodoN, genererà un segnale e terminerà. Il segnale verrà catturato dal thread master, il quale manderà in esecuzione un opportuno gestore dei segnali che non dovrà far altro che effettuare una join per il thread appena terminato, e provvederà a lanciare un nuovo thread **ottieniNodi** che proverà a stabilire una nuova connessione con il NodoN. Se il NodoN ancora non si è messo in ascolto, è stato previsto che il thread proverà sempre a riconnettersi ogni 10 secondi [per maggiori dettagli consultare blockserver.c].

# **Dettagli implementativi del server**

Il server NodoN ha il compito di mettersi in ascolto di una connessione da parte di un BlockServer nel frattempo il nodon avrà un thread che genererà blocchi da aggiungere alla sua blockchain e al file.

Descrivere comunicazione del nodon con il blockserver, con le 3 scelte etc…

Per maggiori dettagli far riferimento al file [nodon.c]

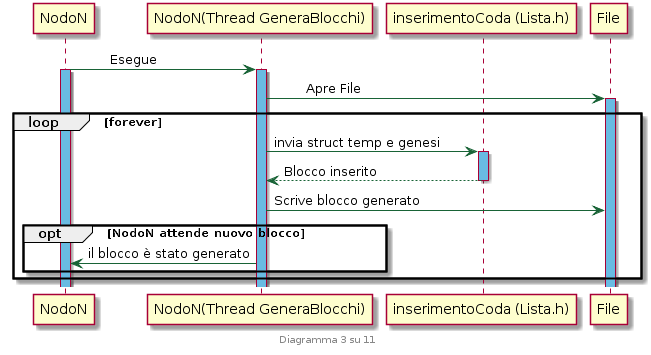
Descrivere parte server del blockserver cioè di come comunica con il blockclient

ATTENZIONEEE!!!!!!!!!!!!!!

Lo schema raffigurato a [Pagina 6] rappresenta per sommi capi le macro-azioni che ogni entità effettua all’interno della rete, verranno approfondite in seguito nel dettaglio. In questo schema vengono descritte le operazioni nell’ordine più consono rispetto alle richieste del progetto, ma la reale implementazione tiene conto delle possibili anomalie che possono far si che alcune azioni non vengano eseguite nell’ordine prestabilito a [pagina 6] .

Da come si evince dalla figura a [pagina 6] la prima azione viene effettuata dal *NodoN* , esso ha il compito generare una blockchain, in seguito il *NodoN* si mette in attesa di connessione di un *BlockServer*, che quando si connette richiede il trasferimento dei blocchi a partire da un blocco specifico. Dopo che il BlockServer ha costruito una propria copia della blockchain, è pronto per accettare connessioni con i *BlockClient* che richiederanno dei servizi per analizzare le transazioni.

## Schema Generazione Blocchi



### Descriziome Generazione Blocchi

Prima di analizzare la generazione di blocchi, è di fondamentale importanza introdurre la struttura dei blocchi e il loro contenuto:

1. **struct** Blocco
2. {
3. **int** n;
4. **int** tempo;
5. **struct** Transazione ts;
6. **struct** Blocco \*next;
7. } ;

n: Rappresenta l’identificativo progressivo dei blocchi, che in questo progetto parte da 0 con il blocco **genesi**.

tempo: Rappresenta un tempo randomico compreso tra 5 e 15 secondi che il NodoN deve attendere prima di inserire un nuovo blocco nella blockchain.

next: Rappresenta un puntatore al successivo blocco, considerando che la blockchain viene rappresentata come una lista.

La transazione ts è a sua volta una struttura così definita:

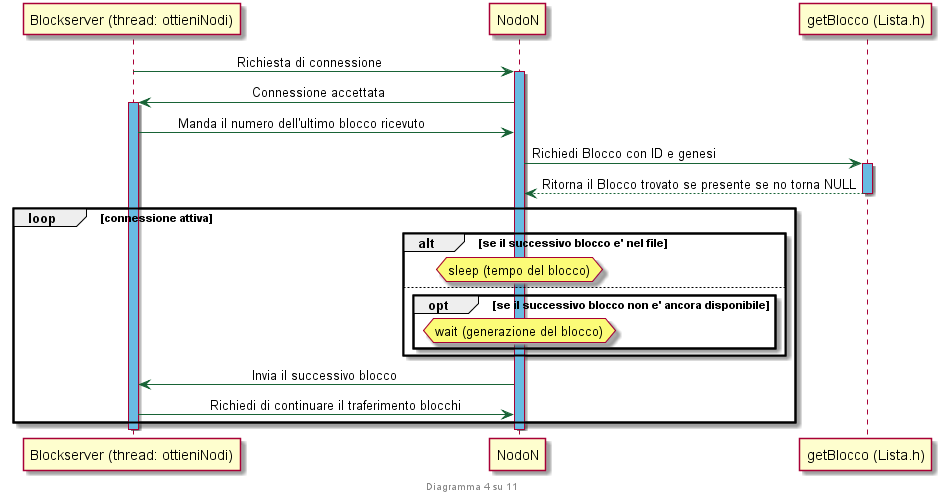
1. **struct** Transazione
2. {
3. **char** ipMittente[16];
4. **int** portaMittente;
5. **int** credito;
6. **char** ipDestinatario[16];
7. **int** portaDestinatario;
8. **int** numRandom;
9. };

Stabilite le strutture che vengono utilizzate, il *NodoN* appea va in esecuzione , lancia il thread produci che si occupa di aprire il file, per un tempo indefinito si occuperà di generare dei blocchi che verranno inseriti in coda alla blockchain e sul file. Una nota particolare va fatta sulla scrittura nel file, poiché ci si avvale di una struttura temporanea per evitare di scrivere dati superflui come il campo “next” della struttura blocco:

1. **struct** temp
2. {
3. **int** n;
4. **int** tempo;
5. **struct** Transazione ts;
6. };

Infine, il thread ha il compito di svegliare suo padre *NodoN* nel caso in cui quest’ultimo sia in attesa di un nodo che il thread ha appena generato.

## Schema Trasferimento Blocchi



## Descrizione Trasferimento Blocchi

Ci si riferisce al thread *ottieniNodi* con il nome del thread master che lo compone: *BlockServer*.

Il *BlockServer* per ottenere i nodi che utilizzerà per le analisi di un generico *BlockClient* si connetterà al *NodoN*, successivamente gli invia l’identificativo dell’ultimo blocco in suo possesso, per far sì che il *NodoN* gli invii i blocchi a partire dal successivo blocco posseduto da *BlockServer*. Dopo la richiesta entrambe le entità entreranno in un loop che potrà essere interrotto solo se una delle due parti si disconnette.

Il *NodoN* controlla l’identificativo che ha ricevuto da *BlockServer*, se questo identificativo corrisponde ad un blocco presente nel file, *NodoN* preleverà questo blocco e attenderà il tempo randomico del blocco, poiché considerando che era stato generato in una precedente esecuzione del *NodoN*, dato che in questa nuova esecuzione non ha atteso il tempo randomico, questo comportamento viene simulato prima di inviarlo al *Blockserver*.

Nel caso in cui sia *NodoN* che *BlockServer* hanno la stessa copia della blockchain, allora il *NodoN* dovra attendere che il thread **produci** generi un nuovo blocco da inviare a *BlockServer*.

Mentre nel caso in cui il blocco viene generato al momento allora non ci sarà nessuna attesa da parte del *NodoN*, poiché si fa fede all’attesa effettuata durante la generazione del blocco.

## Schema Analisi BlockChain

# Descrizione Analisi BlockChain

Le implementazioni delle scelte che si evincono dallo schema a [pagina 14] verranno approfondite nelle corrispettive descrizioni degli schemi.

La richiesta di connessione consiste in una connect verso l’indirizzo del server, a connessione effettuata ambo le controparti avranno a disposizione un descrittore di socket che utilizzeranno per farsi delle richieste.

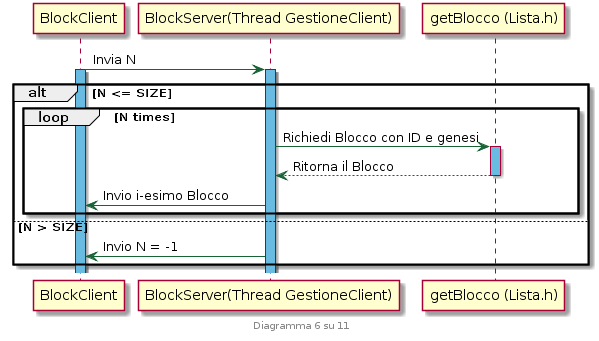
Per ogni connessione con i *BlockClient*, il BlockServer creerà un thread che avrà il compito di gestire tutte le richieste del corrispettivo *BlockClient* ad esso assegnato.

Quindi il thread GestioneClient, fin quando il *BlockClient* vuole richiedere dei servizi, dovrà restare attivo.

Come prima operazione che è stata prevista dal protocollo applicazione, ci si aspetta che il *BlockClient* invii un intero che corrisponderà ad una scelta di un determinato servizio.

I servizi previsti dal protocollo applicazione sono 6, in più è presente una scelta 0 che viene effettuata quando il *BlockClient* vuole terminare l’analisi della blockchain.

## Schema Scelta Uno



### Descrizione della scelta uno

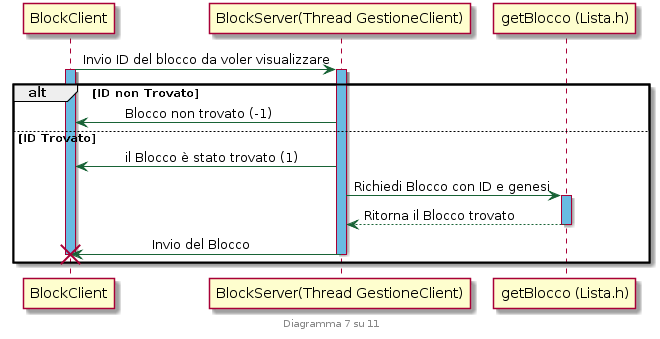
Il BlockClient invierà con una FullWrite un intero N al BlockServer, questo valore corrisponderà al numero degli ultimi blocchi delle blockchain che il BlockClient vuole visualizzare.

Il Thread GestioneClient una volta che riceve N, in mutua esclusione va a controllare se in quell’istante va a verificare se i blocchi richiesti sono presenti nella blockchain con getBlocco, dato che in concorrenza a questo thread viene eseguito anche l’altro thread che aggiorna la blockchain, la mutua esclusione viene adoperata proprio per garantire l’analisi della blockchain in un istante in cui essa non viene aggiornata.

Come risposta alla richiesta, il BlockServer invia i blocchi solo se essi sono presenti nella blockchain e li invia uno alla volta. Nel caso in cui i blocchi non sono presenti nella blockchain il client riceverà un intero (-1) che gli segnalerà l’assenza dei blocchi.

Così come adoperato per la scrittura sul file (vedi pagina 9), anche per quanto riguarda la scrittura dei blocchi su una socket, non viene adoperata direttamente la **struct Blocco**, ma viene utilizzata la **struct temp,** il motivo è sempre da ricondursi all’inutilità di inviare anche il campo **next** della **struct Blocco**, che non è altro che un indirizzo di memoria del BlockServer, di fatto superfluo per il BlockClient.

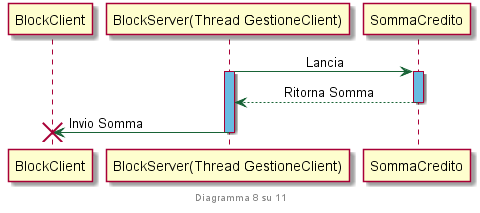
## Schema Scelta Due



### Descrizione scelta due

Il BlockClient invierà, con una FullWrite al BlockServer, un intero che corrisponde all’ID del Blocco che vuole visualizzare, il BlockServer controllerà se il blocco è presente o meno nella blockchain, se tale blocco non è stato trovato allora verrà inviato un intero negativo(-1) al BlockClient, invece se il blocco è stato trovato verrà inviato un intero positivo (1), successivamente con la funzione getBlocco verrà prelevata una copia di quel blocco dalla lista che inizia con il blocco genesi, e successivamente il blocco richiesto verrà inviato a BlockClient sottoforma di struct temp.

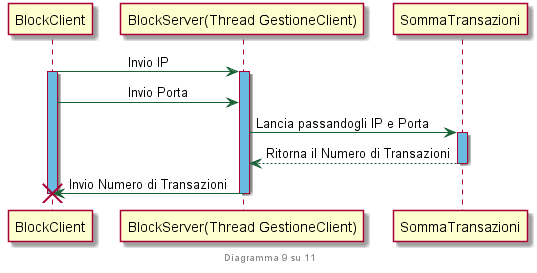
## Schema Scelta Tre



### Descrizione scelta tre

Quando il BlockClient richiede la scelta numero 3, si effettuano le operazioni descritte dal protocollo applicazione nel [Diagramma 8], cioè il BlockServer chiama la funzione SommaCredito che scorrendo tutta la lista, calcolerà con una variabile accumulatore il valore totale di tutte le transazioni, questo valore intero ritornerà al thread chiamante che a sua volta provvederà a inviarlo come valore intero al BlockClient.

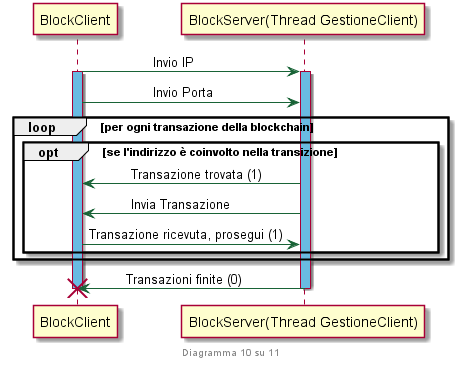
## Schema Scelta Quattro



### Descrizione scelta quattro

Il BlockClient invia con una FullWrite un indirizzo IP sottoforma di array di caratteri, e successivamente invia con una seconda FullWrite un valore numerico Porta, queste due variabili in coppia definiscono uno specifico indirizzo che il BlockServer dovrà cercare all’interno delle transazioni, il BlockServer fa ciò avvalendosi della funzione Somma transazioni, la quale riceve come argomenti proprio l’IP e porta richiesti dal BlockClient e conterà il numero di volte in cui l’indirizzo è coinvolto nella blockchain, sia come mittente oppure come destinatario. La funzione SommaTransazioni ritornerà il numero di transazioni che successivamente il Thread GestioneClient invierà al BlockClient.

## Schema Scelta Cinque



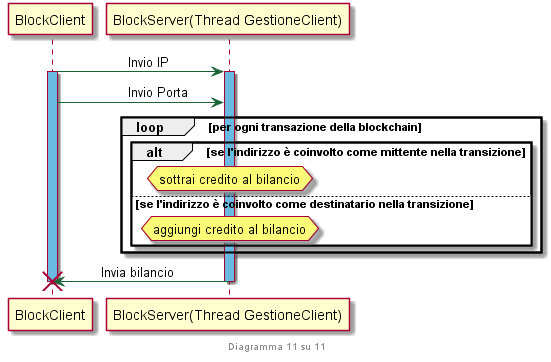
### Descrizione scelta cinque

Il BlockClient invia con una FullWrite un indirizzo IP sottoforma di array di caratteri, e successivamente invia con una seconda FullWrite un valore numerico Porta.

Il BlockServer per ogni transazione della blockchain va a controllare se l’indirizzo è coinvolto nella transazione, se si, invierà al BlockClient il valore 1 per indicare il risultato positivo della ricerca, dopodiché con una seconda FullWrite invierà l’intero blocco avvalendosi della struct temp, infine il BlockServer attenderà con una FullRead che il BlockClient abbia ricevuto l’i-esimo blocco, per poi tornare a cercare l’indirizzo nelle altre transazioni.

Quando tutta la lista è stata controllata, per indicare la terminazione della ricerca, il BlockServer invierà con una FullWrite uno 0 al BlockClient.

## Schema Scelta Sei



### Descrizione scelta sei

Il BlockClient invia con una FullWrite un indirizzo IP sottoforma di array di caratteri, e successivamente invia con una seconda FullWrite un valore numerico Porta.

Il BlockServer per ogni transazione della blockchain va a controllare se l’indirizzo ricevuto dal BlockClient è coinvolto nell’i-esima transazione come mittente o destinatario, nel caso in cui l’indirizzo desiderato risulta essere coinvolto come mittente allora dal bilancio bisogna sottrarre il credito di quella i-esima transazione, invece se l’indirizzo desiderato risulta essere coinvolto come destinatario allora dal bilancio bisogna sommare il credito della i-esima transazione.  
Dopo aver controllato tutta la blockchain, il BlockServer invierà il bilancio al BlockClient con una FullWrite sulla socket.