

**12 ESPERTI PROFILO TECNICO CON CONOSCENZE NELLE TECNOLOGIE DEI
SISTEMI INFORMATICI DISTRIBUITI E A REGISTRO DISTRIBUITO E
DELL'INTELLIGENZA ARTIFICIALE**
(Bando del 2 dicembre 2020 – Lettera A)

Testo n. 2

Tre quesiti su tre delle quattro materie del programma scelti tra gli otto proposti dalla Commissione (due per ogni materia del programma).

1. Programmazione, algoritmi, strutture e modelli dati

QUESITO 1A

Valentina sta organizzando una cena per comunicare una notizia importante. Non potendo, per ragioni logistiche, invitare tutti i suoi amici, decide di invitare un minimo numero di persone tali che ognuno dei suoi amici o è un invitato o conosce almeno una delle persone invitate.

La candidata/il candidato:

- 1) descriva un algoritmo che permetta di trovare una soluzione ottima al problema sopra descritto, e ne illustri il costo computazionale;
- 2) descriva un algoritmo che permetta di trovare una soluzione approssimata al problema sopra descritto con un minore costo computazionale rispetto al punto 1;
- 3) assumendo che gli amici di Valentina siano Anna (A), Barbara (B), Carlo (C), Dario (D), Enza (E), Filippo (F), Gaia (G), tali che:
 - A e B si conoscono
 - A e C si conoscono
 - B e D si conoscono
 - B e G si conoscono
 - C e D si conoscono
 - C e E si conoscono
 - D e E si conoscono
 - E e F si conoscono

descrive l'esecuzione dell'algoritmo proposto al punto 1 oppure dell'algoritmo proposto al punto 2 su tale istanza del problema.

QUESITO 1B

Una scuola consente ai genitori di iscrivere i propri figli online, e contestualmente di scegliere la sezione. Il servizio si basa su una applicazione *web* e un RDBMS, in cui è stata definita la seguente tabella:



```
create table ALUNNO (  
  CODICE_FISCALE char(16) not null primary key,  
  NOME varchar(40) not null,  
  COGNOME varchar(40) not null,  
  INDIRIZZO varchar(500),  
  SEZIONE char(1),  
  [...]  
)
```

Al momento dell'iscrizione, viene inserita una nuova riga, ma solo dopo aver contato sulla stessa tabella, e all'interno della stessa transazione, il numero di alunni già iscritti nella sezione prescelta, per verificare se è stato già raggiunto il numero massimo di iscritti. Al termine delle iscrizioni il preside scopre che per una classe c'è stata un'iscrizione in più rispetto al massimo consentito.

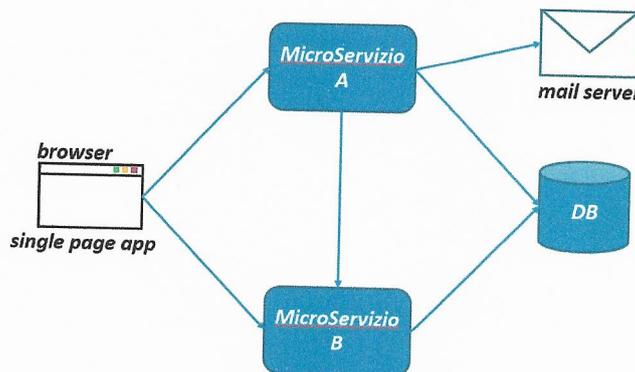
Sulla base di quanto descritto, la candidata/il candidato:

1. introduca i livelli di isolamento secondo lo standard ANSI;
2. descriva l'anomalia verificata, dando una possibile spiegazione al fenomeno;
3. proponga due possibili soluzioni al problema, una basata sull'impiego di un diverso livello di isolamento e una basata su una strategia alternativa;
4. descriva, assumendo di sostituire l'RDBMS con un *database* NoSQL di tipo *key/value* con supporto alla *linearizability*, una possibile soluzione che eviti l'anomalia individuata.

2. Architetture dei sistemi distribuiti

QUESITO 2A

Un'azienda di numismatica ha adottato per il proprio servizio di compravendita di monete su Internet un'architettura a microservizi.



Si richiede alla candidata/al candidato di:

1. definire e descrivere una possibile architettura di autenticazione e autorizzazione in grado di garantire il *single-sign-on*, indicando i punti di intervento sullo schema mostrato sopra e proponendo, se necessario, componenti aggiuntivi;
2. individuare protocolli idonei a consentire l'accesso all'applicazione tramite il proprio *account* Google, Facebook etc. e il recupero dei dati dell'utente cliente (nome, cognome, *email*) da parte dell'applicazione, descrivendo il relativo flusso;
3. proporre una soluzione per rendere sicure le comunicazioni:
 - tra il *browser* e le componenti applicative;
 - tra i microservizi;
 - tra microservizi e servizi di *database* e messaggistica.

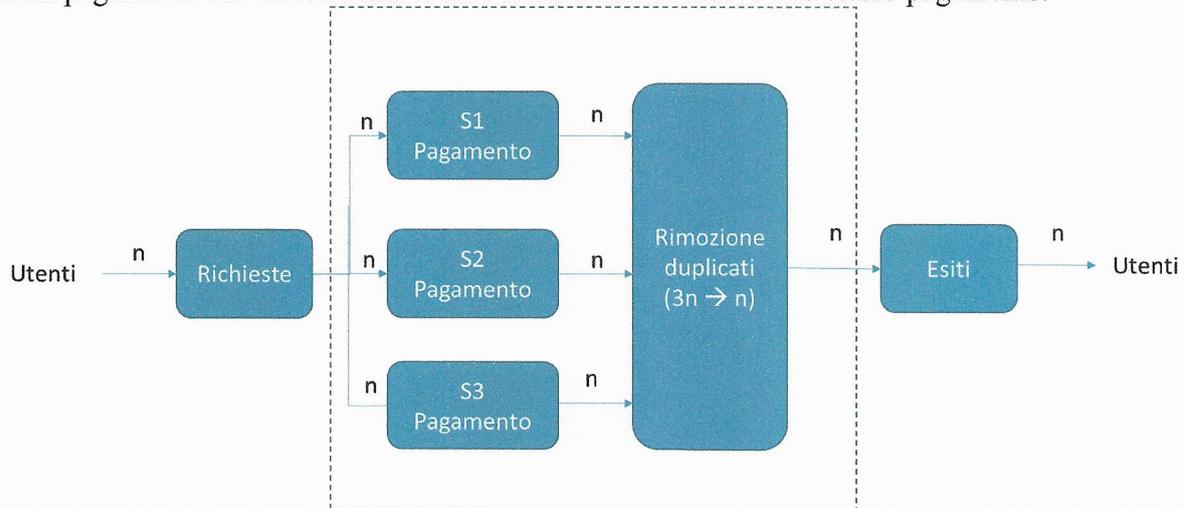


QUESITO 2B

Una banca gestisce un sistema di pagamento che è attivo 24H al giorno tutti i giorni. La parte del sistema dedicata ai pagamenti è costituita da tre *server* che elaborano in parallelo lo stesso flusso ordinato di n richieste in ingresso e producono in uscita ognuno n ricevute di pagamento. Uno stadio di rimozione dei duplicati rimuove le ricevute in eccesso e invia la notifica finale (esito) all'utente.

Il *server* dei pagamenti opera in memoria eseguendo in modo atomico le seguenti due operazioni: una sottrazione sul conto del debitore di un certo importo e una addizione di pari importo sul conto del creditore.

Lo stadio di rimozione dei duplicati opera in questo modo: invia verso lo stadio *Esiti* la prima notifica di un pagamento che riceve e scarta tutte le successive relative allo stesso pagamento.



La candidata / il candidato:

1. descriva le caratteristiche salienti dei sistemi *crash fault tolerant* (CFT) e *byzantine fault tolerant* (BFT);
2. indichi al *fault* di quanti nodi la sezione del sistema composta dagli stadi di pagamento è resistente, motivando la risposta;
3. modifichi la sezione del sistema composta dagli stadi di pagamento e di rimozione dei duplicati per renderla resistente a *fault* di tipo bizantino, specificando il numero minimo di nodi attivi necessari per continuare ad operare;
4. illustri come questa architettura sia in grado di gestire aggiornamenti *software* dello stadio di pagamento garantendo continuità di servizio, motivando la risposta e descrivendo una possibile strategia di aggiornamento che mitighi anche il rischio di disservizio legato a errori nel nuovo *software*.

3. Distributed Ledger Technology e cryptoasset

QUESITO 3A

Con il termine *blockchain* ci si riferisce sia alla particolare struttura dati "a blocchi", condivisa e immutabile, sia all'insieme di tecnologie e protocolli che sono alla base di sistemi, ad esempio *Bitcoin*, che ne sfruttano le potenzialità.

La candidata/il candidato, prendendo come riferimento la realizzazione di un sistema *blockchain* pubblico come *Bitcoin*:

1. descriva il processo di definizione della catena dei blocchi da parte di un *miner*;

2. descriva la gestione dei possibili *branch* da parte dei nodi e il processo di identificazione della *chain* principale di una *blockchain*, chiarendo quando una singola transazione possa essere considerata “confermata”;
3. descriva cosa si intende per *double spending attack* e come questo possa influenzare la definizione della storia di una *blockchain*, arricchendo la spiegazione con la descrizione di un attacco da portare a un sistema con 7 *miners* di *hash rate* equivalente.

QUESITO 3B

Uno *smart contract* permette di concludere rapporti di natura contrattuale fra le controparti attraverso un protocollo informatico che ne automatizza l’esecuzione sulla base di clausole concordate.

La candidata / il candidato:

1. illustri come la *blockchain* rappresenti una tecnologia particolarmente indicata per l’implementazione degli *smart contract*;
2. illustri i vantaggi degli *smart contract* in termini di automazione, trasparenza, disintermediazione e oggettività rispetto ai contratti tradizionali;
3. illustri la proprietà dei linguaggi di programmazione Turing completi utilizzati tipicamente per la scrittura di uno *smart contract* e le differenze con un linguaggio non Turing completo utilizzato, ad esempio, da *Bitcoin*;
4. in riferimento alla piattaforma *Ethereum*, descriva le modalità per attuare un attacco “*stack overflow*” durante l’esecuzione di uno *smart contract* vulnerabile.

4. Intelligenza artificiale

QUESITO 4A

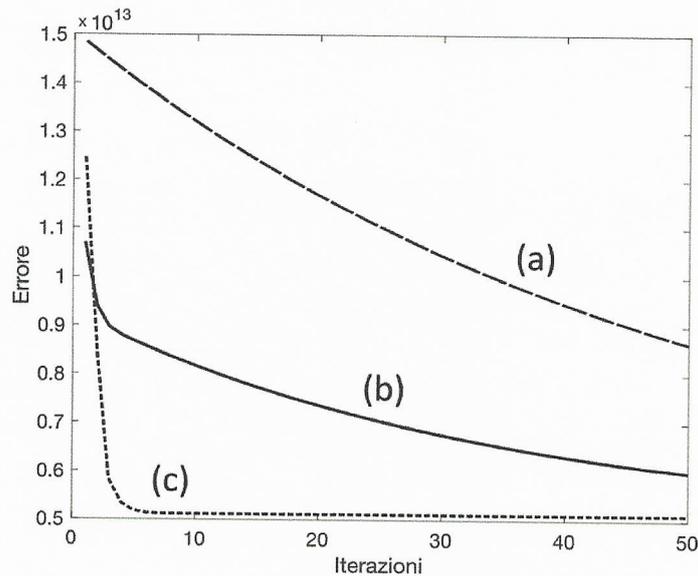
Tecniche di apprendimento automatico o *machine learning* vengono oggi impiegate in un numero sempre crescente di ambiti per varie finalità. A seconda degli algoritmi e della tipologia di problemi affrontati, i modelli che vengono prodotti hanno caratteristiche differenti, ma una caratteristica che li accomuna è la presenza di una fase di “apprendimento” (o “addestramento”) basata sui dati.

In questo contesto, la candidata/il candidato:

1. caratterizzi la classe di approcci all’apprendimento automatico basati sull’errore (*error-based learning*) e descriva sinteticamente un esempio di caso d’uso;
2. descriva l’algoritmo di “discesa del gradiente” (*gradient descent*) per l’apprendimento dei parametri di un modello della classe di cui al punto precedente.

Nell’ambito della realizzazione di una soluzione di *machine learning*, viene utilizzato l’algoritmo di discesa del gradiente per l’apprendimento dei parametri del modello a partire da un insieme di dati già opportunamente preparato. Vengono effettuate tre esecuzioni dell’algoritmo con valori diversi dell’iper-parametro noto come *learning rate*. Il seguente grafico riporta l’andamento dell’errore (*loss*) delle tre istanze su 50 iterazioni:





Sulla base delle curve ottenute nell'addestramento del modello, la candidata/il candidato:

3. indichi quale esecuzione tra (a), (b) e (c) dell'algorithm può ritenersi soddisfacente per l'individuazione dei parametri del modello nell'intervallo di iterazioni considerato, motivando opportunamente la risposta;
4. con riferimento al punto precedente, per ogni esecuzione non ritenuta soddisfacente identifichi le motivazioni che potrebbero aver prodotto i comportamenti osservati.

QUESITO 4B

La candidata/il candidato:

- 1) descriva le caratteristiche salienti delle tecniche di ricerca locale e le loro principali applicazioni in Intelligenza Artificiale;
- 2) descriva in dettaglio un algoritmo di ricerca locale, evidenziandone i principali vantaggi e limitazioni rispetto ad altre tecniche (almeno una).

Si consideri il problema di trovare una configurazione con il minor numero di conflitti in una scacchiera 4x4 con tre regine. Il numero di conflitti di una configurazione è il numero di coppie di regine sulla stessa riga, colonna o diagonale della scacchiera. Una configurazione C2 è vicina ad una configurazione C1 se C2 è ottenuta da C1 muovendo una sola regina in verticale per una sola casella. La candidata/il candidato

- 3) descriva l'esecuzione dell'algorithm di ricerca locale descritto al precedente punto 2, nel caso in cui l'algorithm consideri come soluzione iniziale la seguente configurazione (R1, R2 e R3 sono le tre regine):

R1	R2		R3

Discuta inoltre se la soluzione ottenuta dall'algorithm è ottima.



Prova in lingua inglese

Some say that technology – especially mobile devices – is making people less socially active. Discuss.

