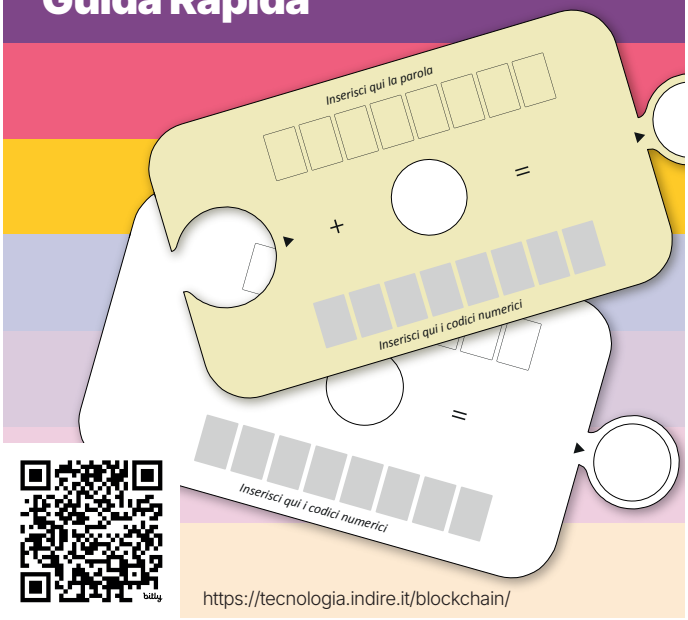
INDIRE ISTITUTO NAZIONALE DOCUMENTAZIONE INNOVAZIONE RICERCA EDUCATIVA

La Blockchain a scuola

Impariamo il funzionamento della Blockchain giocando

Guida Rapida



https://tecnologia.indire.it/blockchain/

Blockchain a Scuola

Un innovativo gioco didattico progettato per rendere accessibili e divertenti i concetti fondamentali della blockchain.

Non sono richieste competenze informatiche, solo la capacità di eseguire semplici calcoli matematici. Attraverso attività pratiche e sfide tra studenti, i partecipanti scopriranno come funziona questa tecnologia e assimileranno i principi base di cittadinanza digitale e sicurezza informatica, comprendendo anche il ruolo dell'Hacker.

"Blockchain a Scuola" trasforma l'apprendimento in un'esperienza memorabile e coinvolgente, dove il vero successo è acquisire competenze di cittadinanza digitale e sicurezza informatica.

1 | Prepara il gioco

I giocatori si dividono in 5 gruppi.

Ogni gruppo riceve:

- **1** tessera Genesi;
- **5** tessere Standard;
- **1** pennarello cancellabile;
- **1** tabella decodifica;
- Inoltre serviranno **carta** e **matite**.

Assegna i ruoli per ogni gruppo

- Calcolatori dell'hash;
- Verificatore;
- Portavoce.

Il facilitatore (l'insegnante) annuncia e scrive alla lavagna la frase.

Ad esempio:

MARIO REGALA SEI MELE A LUCIA

2 | Codifica della Parola

Ogni lettera viene trasformata in numero usando l'alfabeto:

A = 1, B = 2, C = 3, ..., Z = 26

Ad esempio, Il primo blocco (**Genesi**) riporta la parola "MARIO" che diventa:

M(13) + A(1) + R(18) + I(9) + O(15) = 56

L'**Hash-BLOCCO** del primo blocco è 56 che in questo caso corrisponde all'**Hash-OUT**.

Tutti i blocchi a seguire dal primo hanno un **Hash-IN** che corrisponde all'*Hash-OUT* del blocco precedente. Quindi l'*Hash-OUT* dal secondo blocco in poi si calcola sommando **Hash-IN + Hash-BLOCCO**.

Il blocco 1 "MARIO" ha un *Hash-OUT* di 56 e quindi il blocco 2 "REGALA" ha un *Hash-IN* di 56 e un *Hash-BLOCCO di* 44. L'*Hash-OUT* del blocco 2 corrisponde a 100 ovvero 56 (*IN*) + 44 (*BLOCCO*) = 100 (*OUT*). Ripeti per ogni tessera fino alla fine della catena!

3 | Costruisci la blockchain

1. Incastra le 6 tessere partendo da quella Genesi.
2. Su ogni tessera, scrivi una parola della frase (una per tessera, in ordine).
3. Decodifica le lettere in numeri usando la tabella di codifica (A=1, B=2, … Z=26).
4. Calcola l'*Hash-BLOCCO*: somma i numeri della parola.
5. Calcola l'*Hash-OUT*.
   A. Per il blocco Genesi:
      Hash-OUT= Hash-BLOCCO
   B. Per gli altri:
      Hash-OUT= Hash-IN + Hash-BLOCCO
6. L'*Hash-OUT* diventa l'*Hash-IN* del blocco successivo.
7. L'ultimo *Hash-OUT* è l'**Hash-FINALE** della Blockchain.
8. Il Verificatore controlla tutti i calcoli.

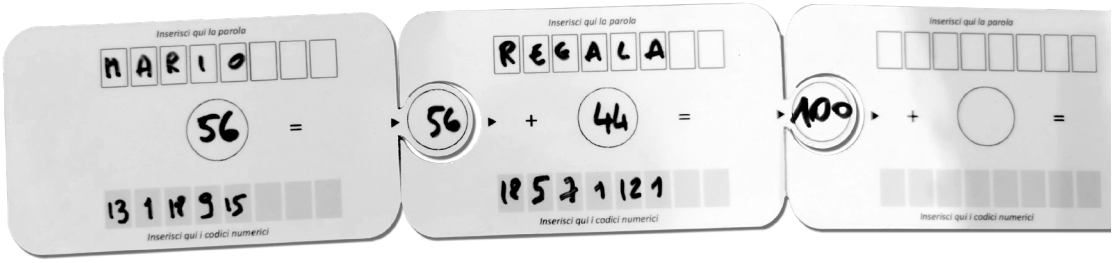
4 | Verifica degli errori

Al termine del tempo stabilito per la costruzione della blockchain, tutti i gruppi si riuniscono per un confronto generale sul valore degli hash-finali.

Poiché tutti i gruppi partono dalla stessa frase, gli hash-finali dovrebbero essere identici, altrimenti, se così non fosse, la maggioranza dei risultati corretti definirebbe il valore esatto della blockchain della frase.

Quindi, se emergono differenze, i Portavoce confrontano i risultati e si avvia una verifica collettiva per individuare gli errori e correggerli, affinché tutte le Blockchain abbiano lo stesso hash-finale.

Se tutto procede in modo regolare, vince la maggioranza, visto che i gruppi sono dispari.



5 | Simula l'attacco

Superato lo step della verifica e correzione degli errori, un partecipante (o l'insegnante) viene nominato **Hacker**.

Si avvia il cronometro, 3min (o 2min, o 1min).

L'Hacker modifica una parola a scelta su una qualsiasi tessera di una catena (ad esempio cambiando "REGALA" in "RUBA") e successivamente, ricalcola tutti gli *Hash-BLOCCO* e gli *Hash-OUT* delle tessere successive a quella modificata.

L'Hacker ottiene così un nuovo *hash-FINALE* che dovrà essere lo stesso nella maggioranza dei gruppi.

L'impresa consiste nel tentativo di hackerare la maggioranza delle Blockchain in gioco prima che il timer segni la fine del tempo stabilito.

6 | Verifica l'integrità

Quando il tempo è finito e il timer ha suonato, tutti i gruppi confrontano nuovamente le parole e gli hash-finali di tutte le Blockchain

Se gli *Hash-FINALE* modificati dall'Hacker non costituiscono la maggioranza, l'attacco è fallito, confermando l'integrità del sistema, altrimenti, l'attacco ha avuto successo e si avvia una discussione per capire le cause.

Il debriefing finale permette di interiorizzare i concetti di immutabilità e consenso distribuito.

Il codice alfabetico