Principles of Cryptocurrency Design

Appunti ed Esercizi

Francesco Pasquale

7 aprile 2025

Nella lezione di oggi abbiamo implementato alcune parti del protocollo *Bitcoin* per generare una catena di blocchi basato su *proof-of-work*. Gli esercizi di questa nota si riferisco al codice scritto in aula (più qualche integrazione), che potete scaricare qui: `https://www.mat.uniroma2.it/~pasquale/dida/aa2425/pcd/pcd250407.zip`

Esercizio 1. Il programma `block.py` genera una sequenza di blocchi a partire dal genesis block di Bitcoin e li scrive su un file `blockchain.dat`. Scrivere un programma che legga il file `blockchain.dat` e verifichi che

1. Ogni blocco contiene nel campo `prev_hash` l'id del blocco precedente;
2. L'id di ogni blocco è inferiore al `target` contenuto nel blocco.

Esercizio 2. Nel codice scritto a lezione abbiamo usato un un `target` costante. Definire un tempo medio `DELTA` che vogliamo imporre fra la creazione di due blocchi consecutivi (diciamo `DELTA = 120` secondi) e un numero `EPOCH_LEN` che corrisponde al numero di blocchi prima di riaggiornare il target (diciamo $\texttt{EPOCH\_LEN} = 60$).

Modificare il codice in `block.py` in modo che, $\texttt{target}(0)$ sia quello del *genesis block* e viene usato per i primi `EPOCH_LEN` blocchi, ma ogni volta che il numero di blocchi creati è $k * \texttt{EPOCH\_LEN}$ per qualche $k \geqslant 1$, per i successivi `EPOCH_LEN` blocchi il target sia dato dalla formula

$$\texttt{target}(k) = \texttt{target(k-1)} \cdot \frac{\delta}{\texttt{DELTA}}$$

dove con δ abbiamo indicato la differenza fra il `timestamp` del blocco $k * \texttt{EPOCH\_LEN}$ e il `timestamp` del blocco $(k-1) * \texttt{EPOCH\_LEN}$.

Esercizio 3. Scrivere un programma che legga un file `blockchain.dat` e, se contiene una catena che soddisfa i due punti dell'Esercizio 1, restituisca la *proof-of-work* della catena, ossia la somma, per ogni blocco, di 2^{256} diviso `target` $+ 1$.

Esercizio 4. Scrivere un programma che legga un file `blockchain.dat` e, se contiene una catena che soddisfa i due punti dell'Esercizio 1, inizi ad aggiungere blocchi alla catena.