Principles of Cryptocurrency Design

Appunti ed Esercizi

Francesco Pasquale

2 maggio 2024

Nella lezione di oggi abbiamo implementato la classe `Script` e un metodo che abbiamo utilizzato per fare il *parsing* degli script. Gli esercizi di questa nota si riferiscono al codice scritto in aula, che potete scaricare qui: `https://www.mat.uniroma2.it/~pasquale/dida/aa2324/pcd/pcd240502.zip`

Esercizio 1. Nel file `script.py` abbiamo implementato un metodo di classe `parse` che prende in input una sequenza di byte opportuna e restituisce l'oggetto codificato nella sequenza. Scrivere un metodo `serialize` che restituisca una sequenza di byte contenente la serializzazione dell'oggetto della classe.

Esercizio 2. Fare il parsing del seguente *locking script* `6e879169a87ca887`. Usando le descrizioni degli OP_CODES[1], determinare cosa dovrebbe contenere un *unlocking script* per ottenere uno script che restituisca TRUE.

[1] Le trovate, per esempio, qui https://wiki.bitcoinsv.io/index.php/Opcodes_used_in_Bitcoin_Script