Principles of Cryptocurrency Design

Appunti ed Esercizi

Francesco Pasquale

9 maggio 2024

Nella lezione di oggi abbiamo implementato la classe `Address` e alcuni metodi che abbiamo utilizzato per generare indirizzi Bitcoin a partire da numeri a 256 bit. 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/pcd240509.zip`

Esercizio 1. A lezione abbiamo implementato il metodo WIF, che restituisce la chiave privata nel formato *Wallet Import Format (WIF)*. Scrivere un metodo di classe PARSE_WIF che legga una stringa in formato WIF e restituisca l'oggetto corrispondente della classe ADDRESS.

Esercizio 2. Abbiamo visto che uno degli indirizzi contenuti negli output script P2PKH della transazione `b35d91a71f226ba961162ca18f321b4d9aada8a0e722430ad3d2d2e4dda9a2c0` ha come chiave privata l'hash `sha256` della stringa `Francesco`. Quella transazione ha 500 output del tipo P2PKH tutti con lo stesso ammontare. Scrivere un programma *brute-force* che cerchi di individuare se in quella transazione ci sono altri indirizzi che hanno come chiave privata l'hash `sha256` di altri nomi.

Esercizio 3. Con la transazione testnet `da9c8ebf9861da00cc0cdfb6b7acc5a082903c67d4e89209005e68b65509eb10` abbiamo inserito nell'output script P2PKH un indirizzo che aveva come chiave privata l'hash `sha256` della stringa `Matteo` e abbiamo visto che quell'output è stato immediatamente speso da qualche bot che sulla rete ha individuato facilmente la chiave privata.

Ottenere dei bitcoin testnet tramite qualche faucet, provare a eseguire delle transazioni verso indirizzi con chiavi private facilmente individuabili tramite brute-force e vedere quanto tempo "resistono" prima che qualche bot ne individui la chiave privata e li spenda.