**Wallets**:

1. משה משתמש בארנק דטרמינסטי. הוא איבד את הארנק וכעת מנסה לשחזר את המפתחות הפרטיים שהיו לו. מה מבטיח שמשה לא ישחזר מפתחות אחרים שלא שייכים לו? הרי נוצר איזשהו שורש כללי למפתחות פרטיים.