ackee blockchain

Summer School of Solana

LECTURE 8

Security on Solana

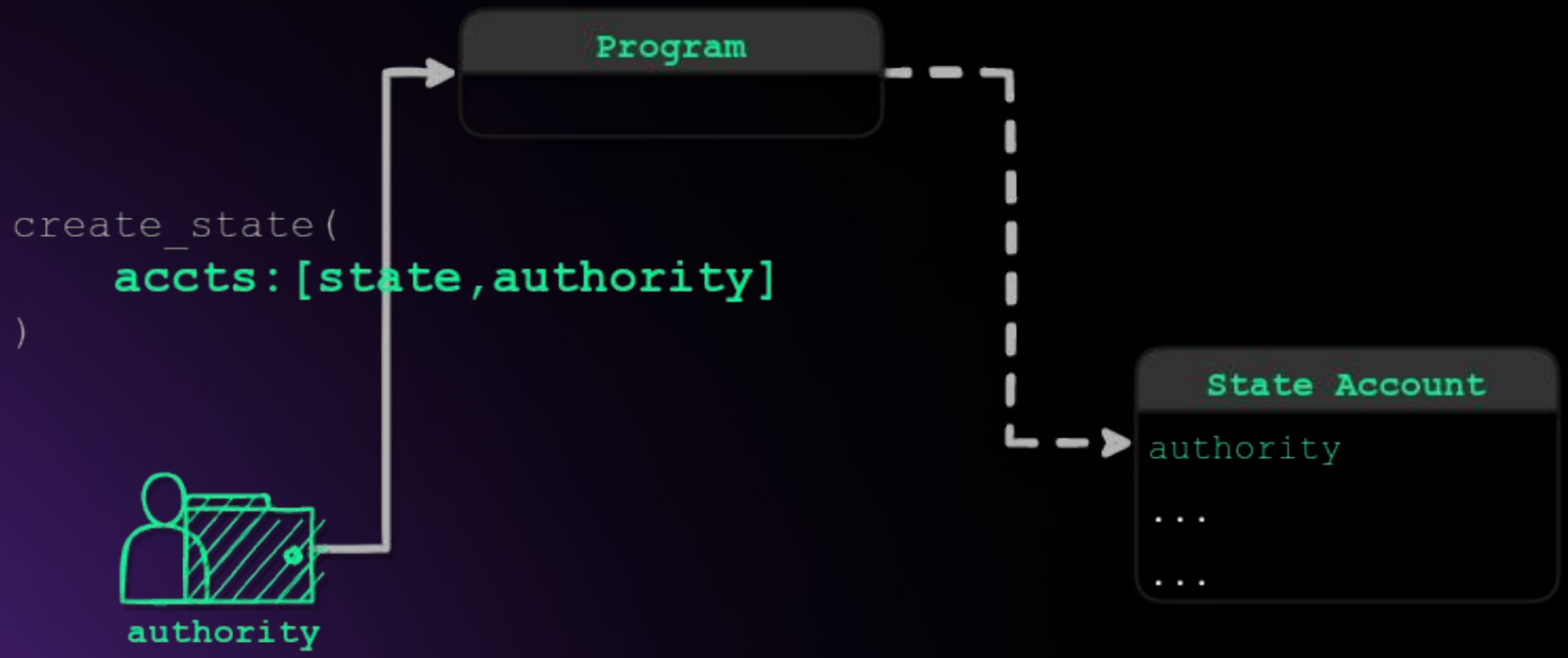
Vladimir Marcin

About this lecture

- **Exploits of common vulnerabilities**
  - Hands-on
  - Anchor + Trdelnik
- **Homework Consulting**
- **Q&A**

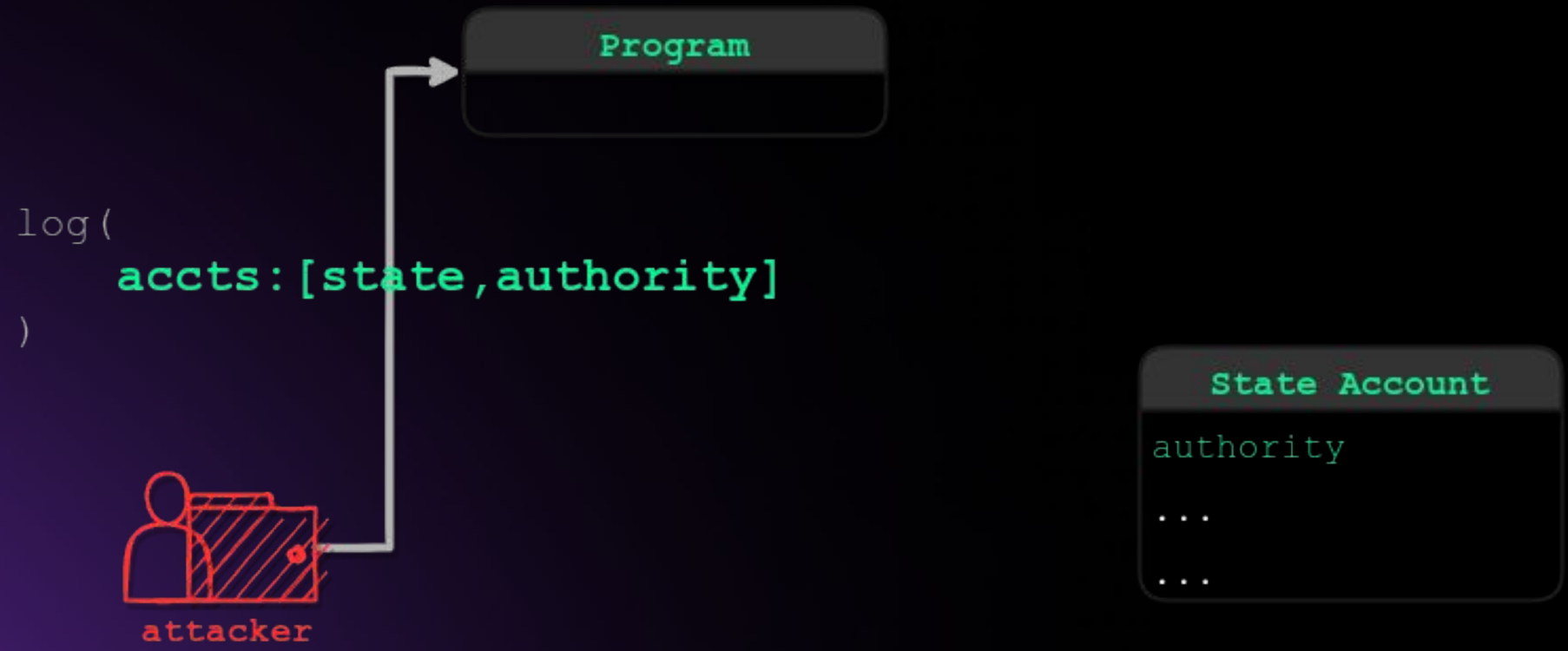
Signer authorization

- If your instruction takes in an authority account, make sure the account has signed the transaction.

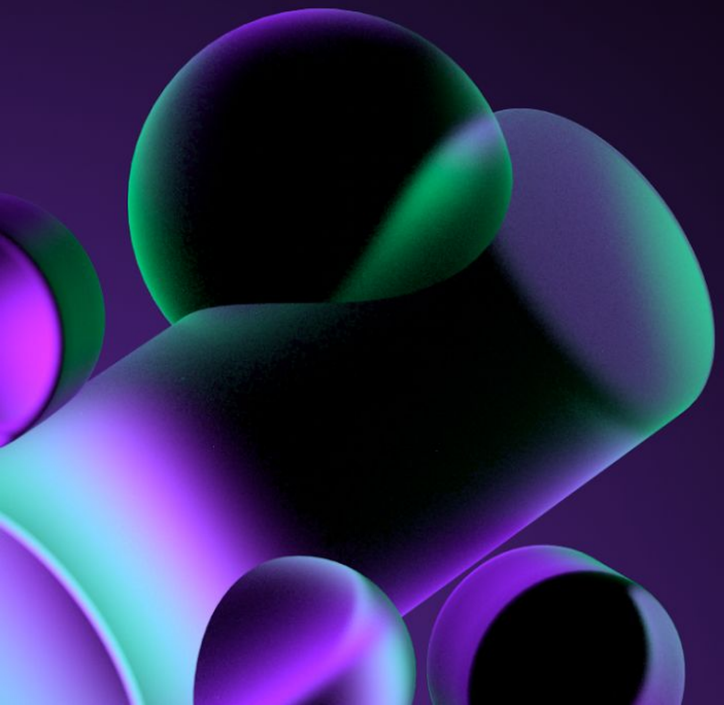


Signer authorization: Attack

- There is only authority instruction in the program. However...

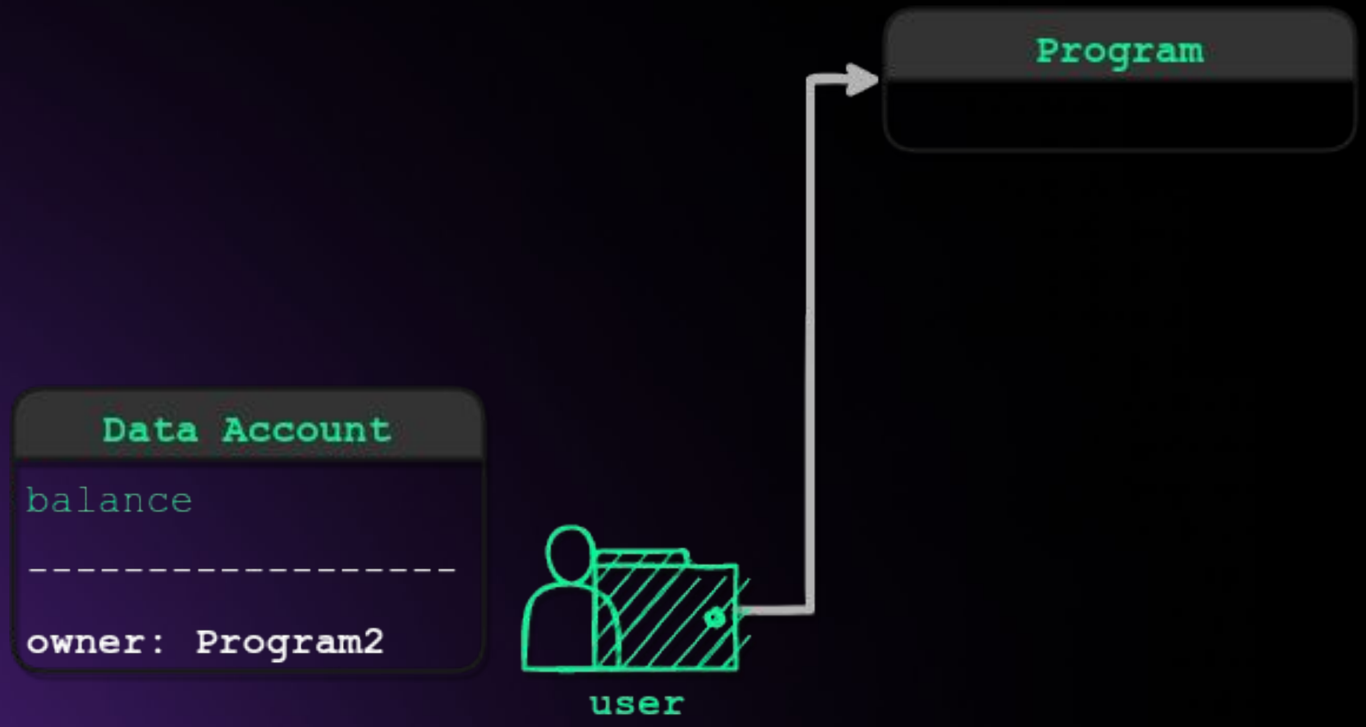


Hands on



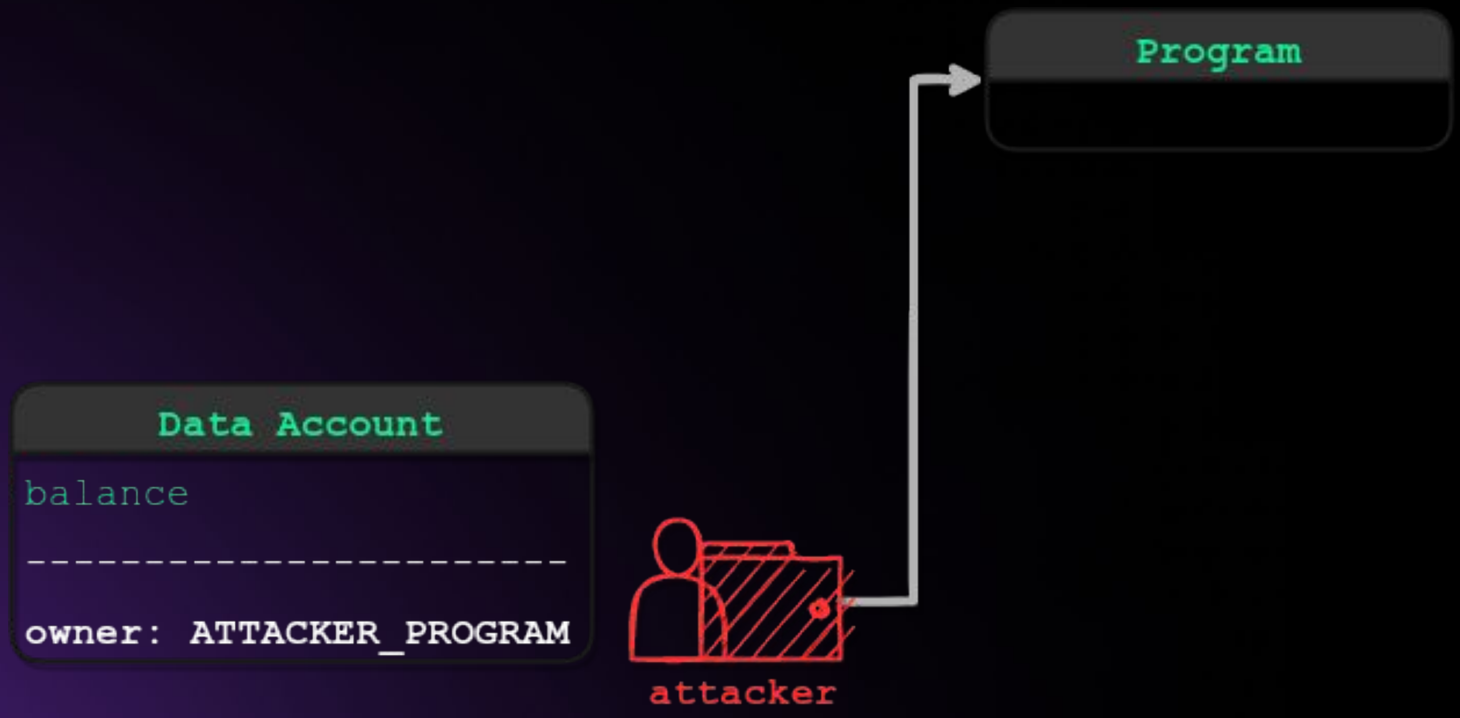
Owner checks

- Make sure the passed-in accounts are owned by the correct program. So you can trust the data in this account.

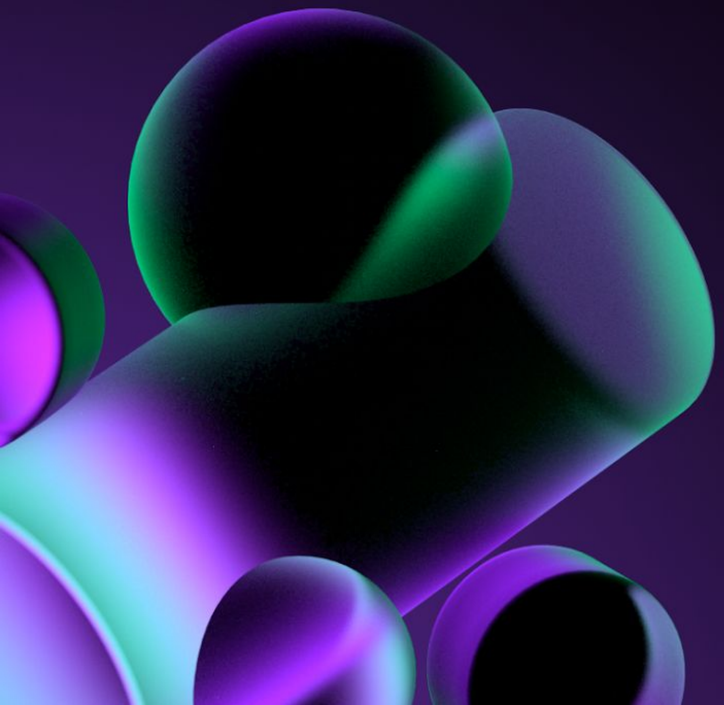


Owner checks: Attack

- If you don't check the owner...

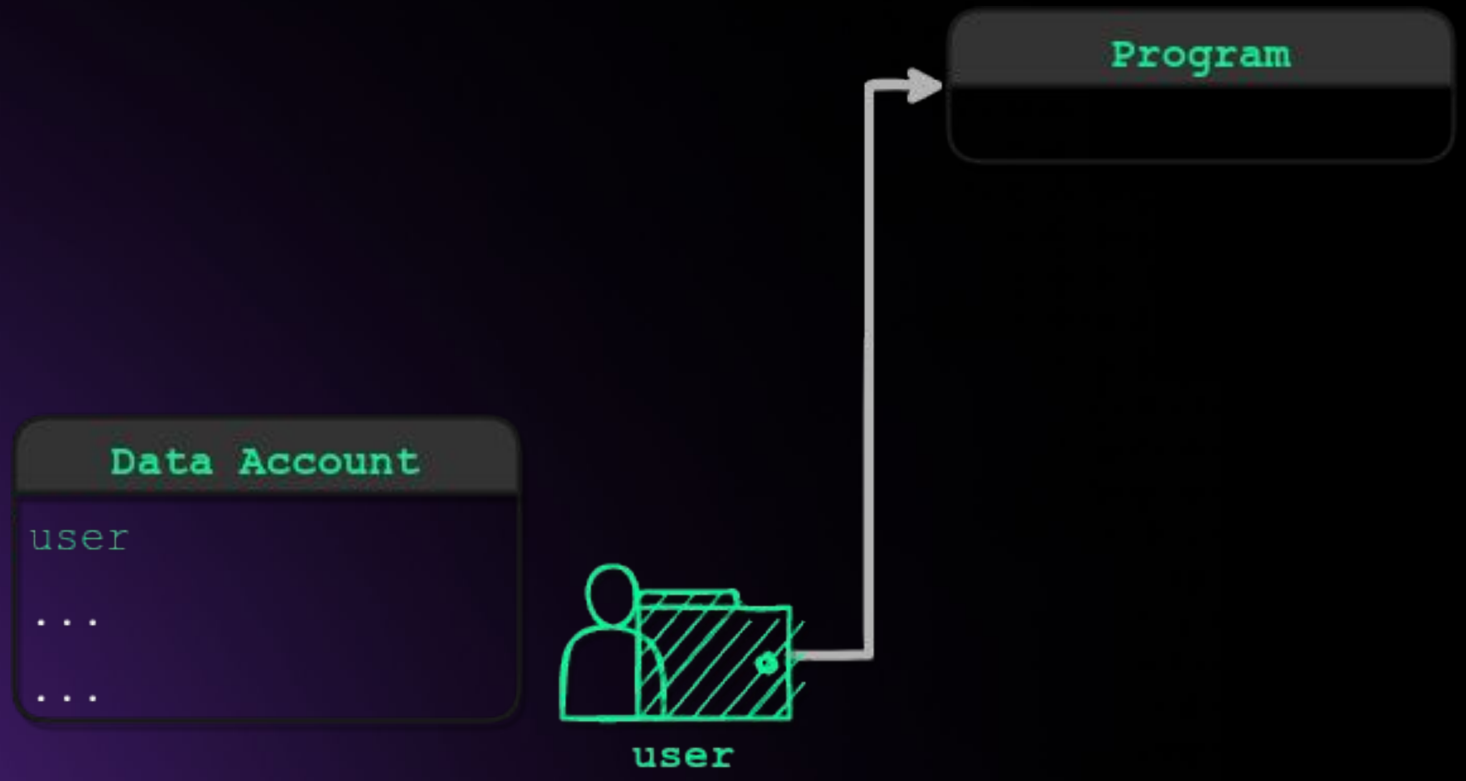


Hands on



Account data matching

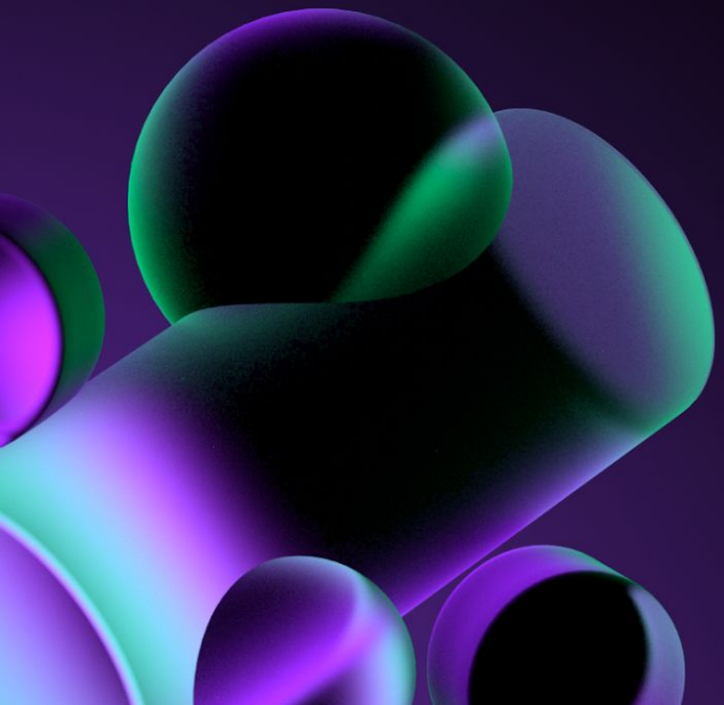
- Make sure that passed-in accounts contain valid data. For example check that a data stored in an account really belongs to the caller.



Account data matching: Attack

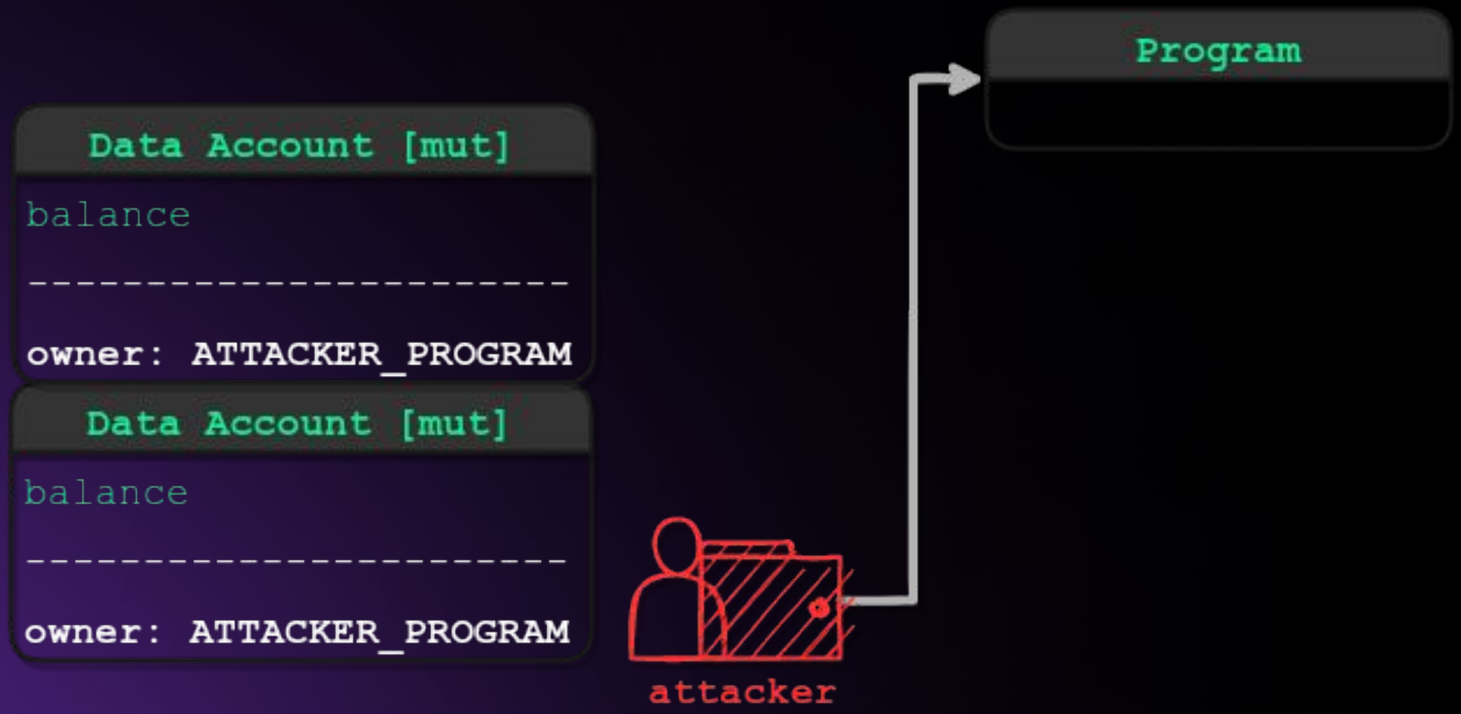
- Make sure that passed-in accounts contain valid data.

Hands on



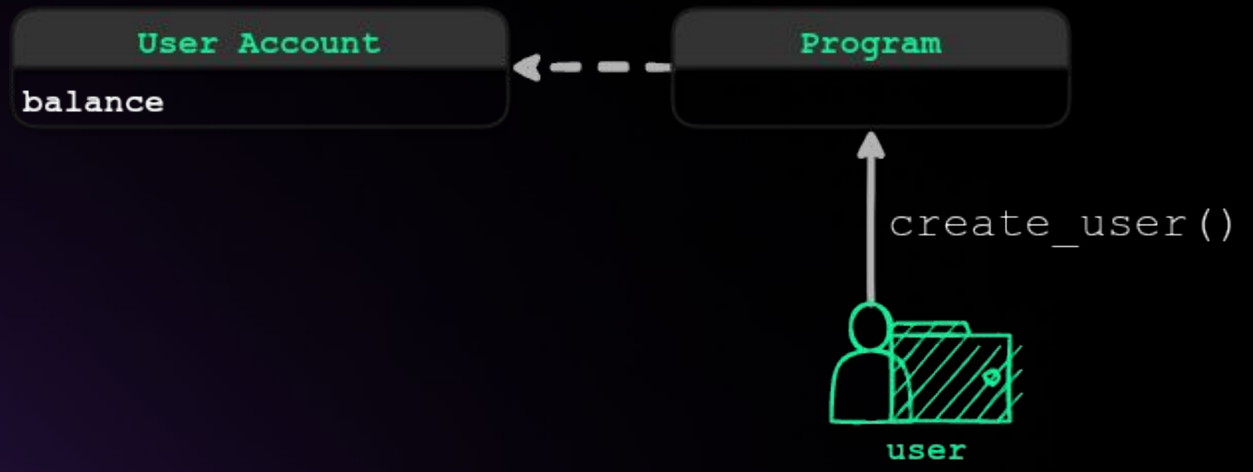
Duplicate mutable accounts

- If your program takes in two mutable accounts of the same type, make sure the attacker don't pass in the same account twice.



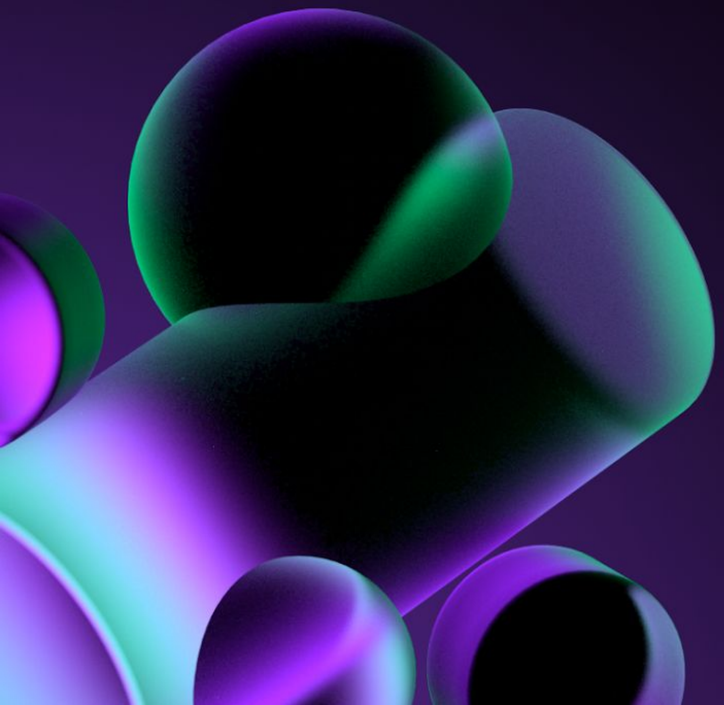
Duplicate mutable accounts: Attack

- Instructions:
  - `createUser`



  - `closeUser`
    - UserA will be closed
    - UserB will receive his/her balance

Hands on

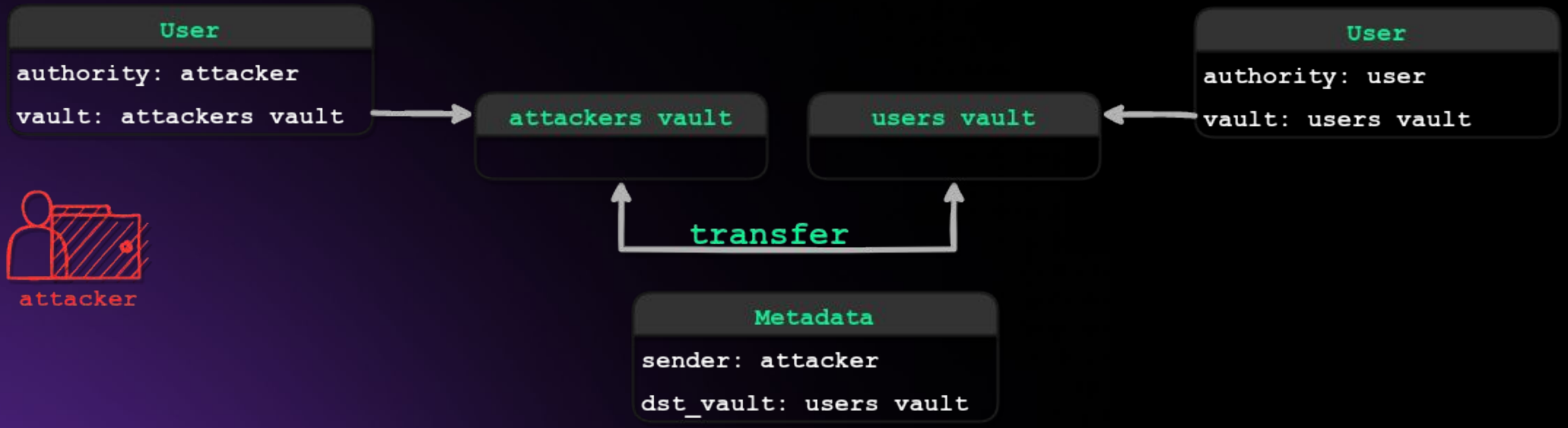


Type cosplay

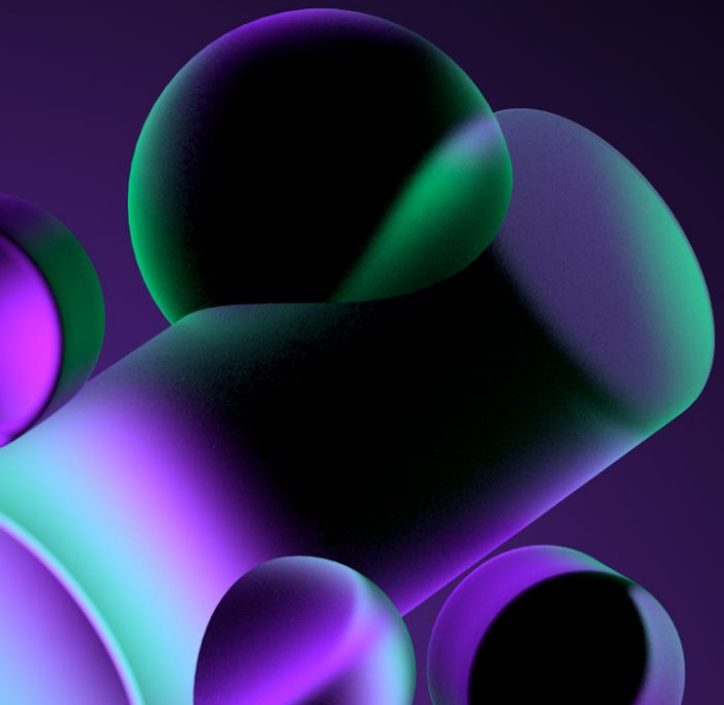
- Make sure one account type (e.g. User) can't be confused for another account type (e.g. Metadata).

Type cosplay: Attack

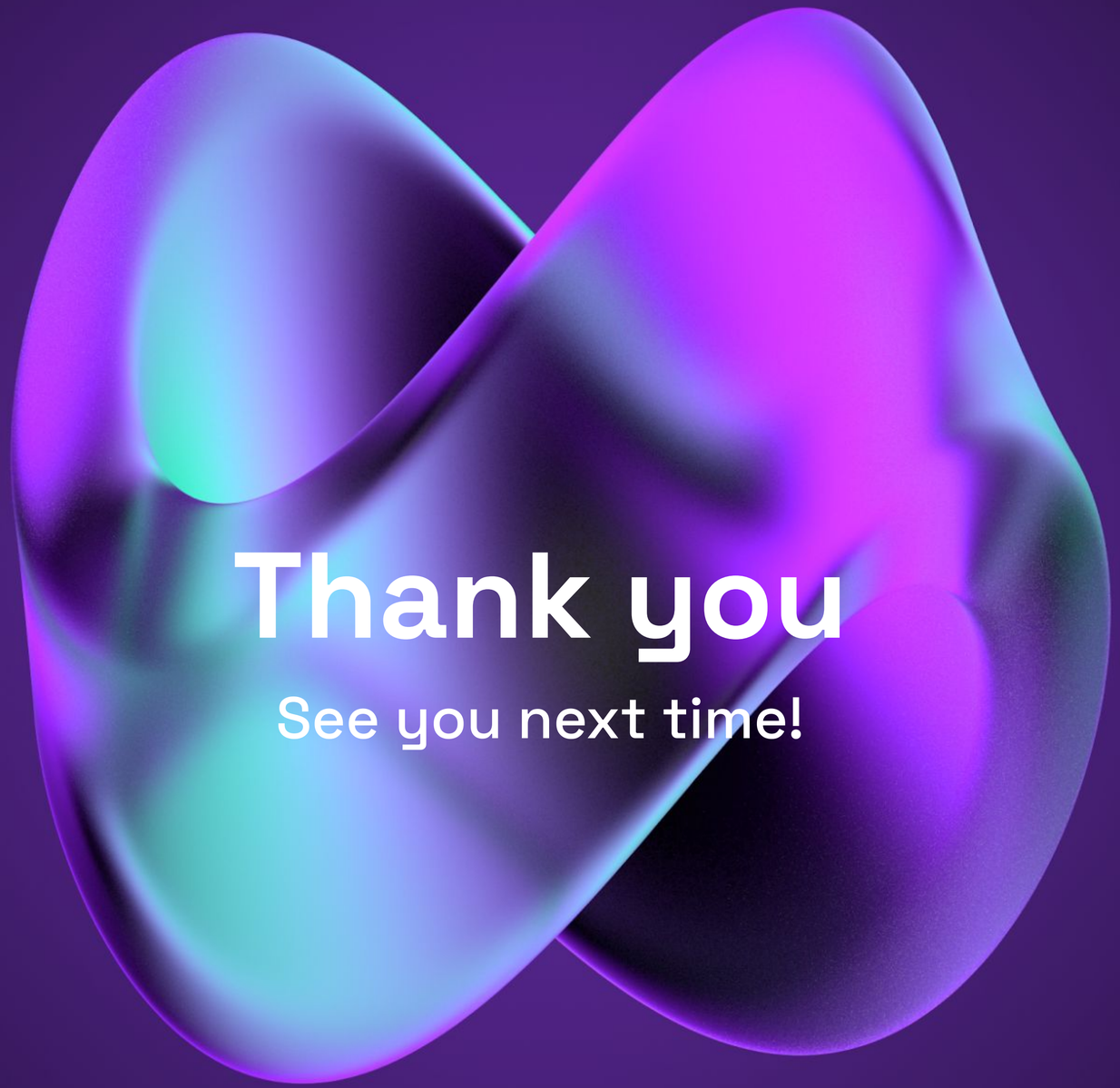
- But...what if it's possible...



Hands on



ackee blockchain



Thank you

See you next time!