ICT3009: Blockchain and Smart Contracts

Due on Fri, February 26th, 2021

Assignment Part 2

Instructions

- This is an individual assignment and carries 15% of the final ICT3009 grade.
- The firm submission deadline is Friday 26th February 2021. Hard copies are not required to be handed in.
- A soft-copy of the report and all related files must be uploaded to the VLE upload area by the same deadline. All files must be archived into a single .zip file. It is the student's responsibility to ensure that the uploaded zip file and all contents are valid.
- Reports (and code) that are difficult to follow due to low quality in the writing-style/organisation/presentation will be penalised.
- You must include all source and any compilation or configuration files and any scripts required to compile and/or run code.

The problem:

- Describe and explain what a `Pay-to-pubkey` (p2pk) UTXO or transaction is and how it works, and describe any problems of p2pk.
- Describe and explain an alternative `Pay-to-pubkey-hash` (p2pkh)
- If you were given, `767695935687`, which is a binary encoding for a Bitcoin script ScriptPubKey, then what ScriptSig would you need to combine the ScriptPubSig with to execute or unlock the ScriptPubKey?
  Hint: 76 → `OP_DUP`
- Figure out what this script is doing: `6e879169a77ca787`