Blockchain Technology Fall, 2023
Tutorial 6, Week 11 (Nov 21)
Due Date: Dec 18

Questions:
1.Suppose you are using the deterministic wallet algorithm introduced in the slides in our course. (1) Please describe how to back up your wallet. Further, suppose the device where your wallet is installed is broken down due to hardware problems. (2) Please describe how to recover your wallet on a new device.**(50 points)**
2. Please study the Full version of Hierarchical Deterministic Wallet in BIP32 (as attached), which give concrete details and attempts to solve the attacks mentioned in our course, e.g., collusion between an auditor and a treasurer. Will you be an advocator or objector of the Full version of BIP32 algorithm? Please justify your answer.**(50 points)**
BIP32 standard, https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki