University of Edinburgh	*Fall 2020-21*
Blockchains & Distributed Ledgers	*Instructor:* Aggelos Kiayias *Teaching Assistant:* Dimitris Karakostas

Assignment #1 (Total points = 100)

Due: Monday 12.10.2020, 16.30

Part 1: Theory (4 x 15 points)

1. How are hash functions used in the context of Bitcoin? Name at least two different ways in which they are used.
2. Derive the formula for the birthday paradox (show your work, explaining every step) and calculate the number of elements needed to find a collision with at least 50%. Apply this to find out how many Bitcoin users are needed to initialize their wallet, which is based on a random selection of 12 random words from the list in https://github.com/bitcoin/bips/blob/master/bip-0039/english.txt, to have the event that at least two users end up with exactly the same secret-key have probability at least 50%.
3. A miner creates a block B which contains address α, on which he wants to receive his rewards. An attacker changes block B, such that instead of α it defines a new address α', which is controlled by the attacker. Will the attacker receive the rewards that the miner tries to claim and why (or why not)? Give a detailed explanation.
4. Describe a functionality which can be implemented with type 2 hierarchical deterministic wallets but not with type 1. (A brief description of hierarchical wallets as well as type-1 and type-2 wallets is available here.)

Part 2: Hands-on (10 + 30 points)

1. Using the course's private Ethereum chain, send 1 ETH to the address of a fellow student. Write a small description on how you conducted the payment, including the transaction's id and addresses which you used. (Instructions on how to connect to the course's private chain are available here)
2. A smart contract has been deployed on the course's private chain. You may find its code here and its deployed address is: *0xcfec964875f363045F19D1dd4c66B3f03B6B2DF5* You can compile and interact with it using Remix. You should create a transaction that interacts with the contract, either depositing to or withdrawing from it some coins. Describe briefly the contract's functionality and provide the id of the transaction you performed and the address you used.