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

Assignment #2 (Total points = 30)

Due: Monday 2.11.2020, 16.30

Smart Contract Programming Part I: Morra

This assignment will focus on writing your own smart contract to implement the Morra game. The contract should allow two players (A, B) to play a game of Morra at any point in time. Each player picks a number between 1-5 and also guesses which number their fellow player has picked. They both show their hands and, in case only player A guesses correctly, A wins and is rewarded x Ether, where x is the sum of the numbers both players picked (similarly if B wins). After the game ends, users should be able to initiate a new game on the same contract.

You should implement the smart contract and deploy it in our private Ethereum ledger. After deploying your contract, you should engage with other students' contracts; you may use Piazza to find a partner. Before you engage with a fellow student smart contract you should evaluate their code and analyze its features in terms of fairness (refer to Lecture 04).

You should submit a PDF report that contains:

- A detailed description of the high-level decisions you made for the design of your contract, including (but not limited to):
  - When and how is the deposit amount of each game decided and committed?
  - How are the winnings sent to the winner?
  - What happens in case of a draw?
- A detailed gas evaluation of your implementation, including:
  - The cost of deploying and interacting with your contract
  - Whether your contract is fair to both players or whether one has to pay more than the other
  - Techniques to make your contract more cost effective and/or fair
- A thorough listing of potential hazards and vulnerabilities that can occur in the smart contract. Provide a detailed analysis of the security mechanisms that can mitigate these hazards.
- A description of your analysis of your fellow students' contracts, including:
  - Any vulnerabilities discovered?
  - How could a player exploit these vulnerabilities to win the game?
- The transaction history of an execution of a game of Morra.
- The code of your contract.