Page	2	3	4	5	6	7	8	9	Total
Mark									

FIRST NAME	
LAST (FAMILY) NAME	
STUDENT NUMBER	

INSE 6630 Final Exam

Fall 2017

Duration: 3 hours
One single-sided letter-sized reference sheet of paper is allowed
Write answers in the provided space
Clearly mark answers that continue on the back of the following page

Each of the following applications are proposed for implementation in Solidity on Ethereum. For each, say whether the functionality that the designer wants is possible to achieve with Ethereum or not and state a (short) reason.

(2 marks) Eve wants to develop a decentralized application that has Alice's public key and pays a bounty to the *first* user that submits Alice's private key (encouraging someone to hack Alice). The app knows a submitted private key value is correct by computing the public key from it and matching it to Alice's.

Circle one:	Possible	Not Possible
Reason:		

(2 marks) Alice wants a decentralized game that can only be played by users who have one of five Ethereum addresses specified in the contract.

Circle one:	Possible	Not Possible
Reason:		

(2 marks) Alice wants a decentralized voting application that collects votes. When users submit votes, she wants to pay the gas costs from her own account and not have the users pay.

Circle one:	Possible	Not Possible
Reason:		

(2 marks) Alice wants a gift application that holds 1 Ether and automatically transfers this money to Bob's Ethereum address on New Year's Day.

Circle one:	Possible	Not Possible
Reason:		

(2 marks) Alice wants an application that generates a log entry each time a payment is sent to the address of this application.

Circle one:	Possible	Not Possible
Reason:		

(2 marks) Alice wants a decentralized lottery application that will let users buy tickets: the tickets are issued with sequential ticket numbers. Alice can then call a function to stop selling tickets, choose a random number from the set of issued tickets, and payout the winning ticket with Ether that is in the contract.

Circle one:	Possible	Not Possible
Reason:		

(2 marks) Alice's application tips the miner who mines the block constructing it.

Circle one:	Possible	Not Possible
Reason:		

(2 marks) Alice's contract can return all Ether it holds to Alice's personal address but she can only receive it if she calls the function after the end of the fiscal year (March 1, 2018).

Circle one:	Possible	Not Possible
Reason:		

This question is a midterm Re-'hash'

(4 marks) A recent bitcoin transaction from Alice to Bob contains two inputs: `In1=1.55` BTC and `In2=0.84`. It has three outputs: `Out1=1.00` and `Out2=1.00` and `Out3=0.38`. How does the UTXO pool change, with respect to the two inputs and three outputs, from before this transaction is broadcast to after it is confirmed in a block?

Answer:

(2 mark) Does the fact that Alice left the miner a tip also change the UTXO pool?

Reason:

(4 marks) Alice is mining Bitcoin. She frequently finds a winning block before she hears of any other winning block, and yet the network tends to build on the other block instead of her's. Assume her block is valid. Provide two realistic reasons why this might be the case.

Reason 1:
Reason 2:

(2 marks) Do all miners in Bitcoin have the same mempool?

Circle one:	Yes	No
Reason:		

(3 marks) Alice lends Bob 1 Ether. Bob is supposed to repay the loan in 1 year with interest. What is the present value of this loan? Give one reason why this loan could become worth more than 1 Ether is worth today, and two reasons why it might become worth less than 1 Ether today.

Reason the loan is worth **more than** 1 Ether:
Reason the loan is worth **less than** 1 Ether:
Reason the loan is worth **less than** 1 Ether:

(3 marks) Carol starts an Ethereum exchange service with $1000 and 2 Ether. Bob deposits 2 Ether, Alice deposits $400, and Bob sells 1 Ether to Alice for $400. Mallory hacks into the exchange and steals 1 Ether from its hot wallet.

(a) Draw the balance sheet of the exchange service.

(b) Is it solvent?

Answer:

Alice has received 5 BTC at a donation address she has published on the web. She wishes to donate some of it to Bob's donation address but does not want Bob to know it was from her.

(2 marks) Alice creates two new accounts: A1 and A2. She sends 4 BTC to account A1 and 1 BTC to account A2. She then sends 1 BTC from A2 to Bob. Can Bob determine this payment is from Alice?

Answer:

(2 marks) Alice finds her friends Carol and David. The three of them create a transaction to which they each input 1 BTC. They output 1 BTC to three new addresses, including an address owned by Alice called A3. Alice then pays Bob from A3. Can Bob determine this payment is from Alice?

Answer:

A smart contract is constructed with an instance variable of: `uint x = 0;`
It contains the following two functions:

```
function test1(address addr){ addr.transfer(10); x=1; }

function test2(address addr){ addr.send(10); x=2; }
```

(1 mark) What does test1 do?

Answer:

(1 mark) What is contained in the variable x after calling test1 on a contract address where the fallback function consumes too much gas for transfer()?

x =

(1 mark) What is contained in the variable x after calling test2 on a contract address where the fallback function consumes too much gas for send()?

x =