Page	2	3	4	5	Total
Mark					28

FIRST NAME	
LAST (FAMILY) NAME	
STUDENT NUMBER	

INSE 6630 Midterm Test

Fall 2017

Duration: 1 lecture period
One single-sided letter-sized reference sheet of paper is allowed

(4 marks) Alice is a surprised millionaire, having purchased Bitcoin when it was not worth much. She is now very concerned about how she will store her bitcoin signing key. Her wallet stores her keys in a file called `wallet.dat` and asks if she'd like to password protect it.

Describe one benefit of using a password-protected wallet
Answer: * malware / theft / etc.

Describe one drawback of using a password-protected wallet
Answer: * lose passwords → lose money.

If Alice wants to keep a backup of her wallet on a USB key in her safe, how should she do this?
Answer: * backup regularly / after new keys / etc

If Alice wants access to her Bitcoin from both her computer and her phone, what type of wallet should she use?
Answer: * online wallet.

if payment, use one input.

(2 marks) A recent bitcoin transaction from Alice to Bob contains two inputs: `In1=1.45` BTC and `In2=0.94`. It has two outputs: `Out1=1.61` and `Out2=0.77`.

Likely owner of Out1 (*circle one*)	Alice	Bob
Likely owner of Out2 (*circle one*)	Alice	Bob

(4 marks) For the above transaction from Alice to Bob, answer the following questions.

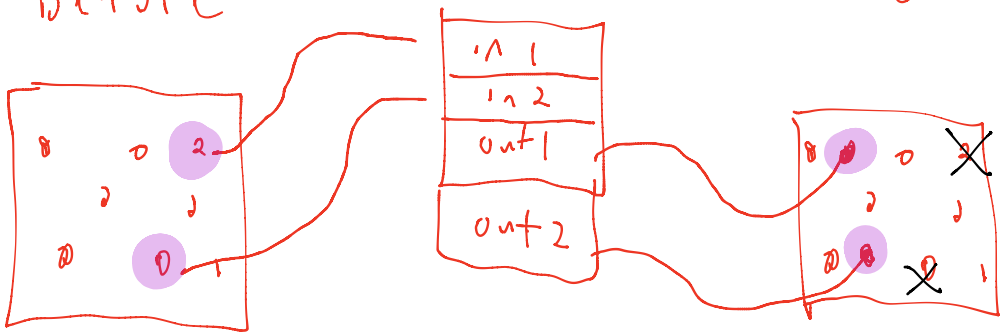
Who else is paid?	(1) Miner
What is the amount?	(1) $\Sigma_{in} - \Sigma_{out} = 0.01$ BTC
Where is this payment recorded?	* transaction (1) * coinbase transaction (1) * block that includes transaction

(4 marks) How does the UTXO pool change, with respect to `In1`, `In2`, `Out1`, and `Out2`, before this transaction is broadcast and after it is confirmed in a block?

Answer:

UTXO Pool

Before



After

(1) In 1/2 before

(1) Removal of in1/in2

(1) addition of out1/2

(1) pointer from in to out.

(3 marks) Alice is using a mobile wallet that uses simple payment verification (SPV). Alice is waiting on a transaction she expects to see from Bob's bitcoin address. Can a malicious SPV node make Alice believe she received it when in reality Bob never sent the bitcoin?

Circle one:	YES	NO
Reason: Node can't fabricate Bob's signature		

(3 marks) Can the malicious SPV node make Alice believe the transaction was never sent while in reality it was sent and confirmed?

Circle one:	YES	NO
Reason: Drop the transaction		

(3 marks) Bob makes a payment to Alice but then sends a competing transaction that sends the money back to himself. This second transaction is confirmed. Can the SPV node make Alice believe the original transaction was confirmed instead?

Circle one:	YES	NO
Reason: * has signature * no work will be added to block not in blockchain → Blockchain. not both.		

B→A B→B

(5 marks) Alice is a Bitcoin miner and is currently trying to solve the proof of work for Block #500000. While she is working, she learns that someone else solved Block #500000.

Should Alice continue to work on 500000 or switch to working on 500001? Explain her rational for this decision.

Switch: * Pr [solving 500000] = Pr [500,000]

* Pr [her 500000 is longest chain]

< [other 500000]

* Lose foot race to having her 500,000 included

Assume Alice finds the solutions for 500000 before she hears of anyone else solving it. Should she broadcast her solution immediately or hold onto her solution to give her an advantage at solving 500001?

* selfish mining

* ≥ 25% computational power