This is a 75 minute, CLOSED notes, books, etc. exam.
ASK if anything is not clear.
WORK INDIVIDUALLY.
Strategy: Scan the entire exam first. Work on the easier ones before the harder ones. Don't waste too much time on any one problem. Show all work on the space provided. Write your name on each page. Check to make sure you have 7 pages.

Question	Points	Score
1	5	
2	5	
3	5	
4	5	
5	5	
6	20	
7	15	
8	5	
9	10	
10	5	
11	10	
12	10	
Total:	100	

1. (5 points) Select **all** of the following true statements about the properties and uses of money.
   - A. Money is *limited in supply* if the supply of it stays relatively constant.
   - B. *Fungible* means that a currency can be divided into smaller units of value.
   - C. Money can be used as a store of value or as a medium of exchange.
   - D. Money should be *durable* so that it can be used many times.
   - E. If a currency is *acceptable* it means that it is easy for individuals to carry with them.

2. (5 points) Select **all** of the following true statements about Okamoto and Ohta's properties of an ideal cryptocurrency.
   - A. If a cryptocurrency guarantees *privacy*, it means that no outside parties will know the identities of clients involved in a transaction.
   - B. *Security* refers both to preventing *forgery* and *double-spending attacks*, where a client uses the same coin in two different transactions.
   - C. Many researchers have pursed the goal of *off-line payment* for a centralized cryptocurrency, where a client can pay a merchant with a cryptocurrency even though the bank is offline. However, satisfying this goal has proved difficult, and many speculate that it may be impossible.
   - D. *Transferability* is an important goal of DigiCash's design. Alice can buy a coin from the bank, buy services from Bob, who can in turn use it to buy services from Charlie, and so on.
   - E. Bitcoin does not offer *independence*, since transactions cannot be sent over computer networks.

3. (5 points) Select **all** of the following true statements about the blockchain.
   - A. Blocks in a blockchain must contain (at a minimum) some data, some form of Sybil resistance, and a cryptographic hash linking it to the previous block (if there is a previous block).
   - B. The *genesis block* is the most recent block in the blockchain that all miners have agreed upon.
   - C. A block is considered *finalized* in the Bitcoin blockchain once it is impossible for the miners to rollback to any previous block.
   - D. A blockchain can be thought of as a tree, albeit with mostly dead branches.
   - E. The blockchain can serve as a *immutable ledger*; different protocols can be used to take advantage of this fact by writing transactions to store critical details in the blockchain's history.

4. (5 points) Select **all** of the following true statements about distributed computing.
   - A. *Partition tolerance* means that all nodes in a network should have the same shared state.
   - B. The Byzantine General's problem discusses the challenges of establishing distributed consensus when messages may be dropped, deleted, or changed.
   - C. Distributed protocols can usually guarantee either consistency or availability, but not both.
   - D. Bitcoin prioritizes consistency and partition tolerance, at times sacrificing availability.
   - E. *Partition tolerance* is generally less important than either consistency or availability for distributed protocols.

5. (5 points) Select **all** of the following true statements about cryptocurrency wallets.
   - A. A wallet is a collection of public key/private key pairs; if the private keys are compromised, anyone could spend the funds they control.
   - B. When creating a mnemonic, you must choose a passphrase; if the passphrase does not match the generated list of words, the user will be given an error message.
   - C. JBOK wallets rely on a mnemonic string of words to preserve a seed without storing it on a user's computer.
   - D. Bitcoin initially used only seeded wallets; keys were generated randomly and stored on the user's hard drive.
   - E. One option for storing funds more securely is to use a *paper wallet*; since the funds are not stored on the user's hard drive, the keys cannot be stolen by malware.

6. (20 points) Consider the inputs and outputs for a single transaction from a Bitcoin-like protocol:

```
Inputs:                                 Outputs:
{txID: '82139f', outputIndex: 0,        { address: 'f342', amount: 20 }
       pubKey: PK1, sig: SIG1}          { address: '08a7', amount: 42 }
{txID: 'c042ee', outputIndex: 3,        { address: '1202', amount: 99 }
       pubKey: PK2, sig: SIG2}          { address: 'efa1', amount: 18 }
```

Also, the mapping of UTXOs is:

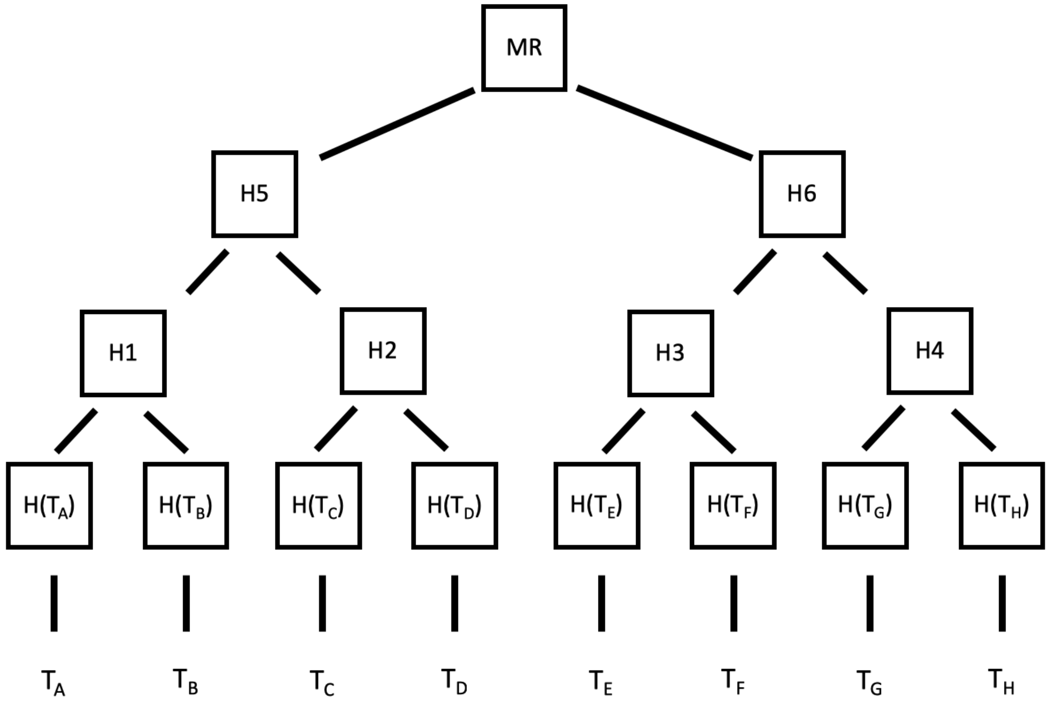
```
utxos['82139f'][0] = { address: '194A', amount: 150 }
utxos['1b29c7'][0] = { address: '9921', amount: 31 }
utxos['c042ee'][1] = { address: '0a3d', amount: 18 }
utxos['c042ee'][3] = { address: 'fa12', amount: 52 }
utxos['41bd70'][0] = { address: '007a', amount: 218 }
```

(a) What calculations would you need to do to determine whether this transaction is valid? (Assume that you have a `hash` and a `verifySig` function available; the arguments can be in whatever order you wish, as long as all needed information is passed in to the function).

(b) What is the transaction fee for this transaction?

(c) If the ID of the above transaction is `"fae123"`, what will the UTXOs be after a miner accepts this transaction and the block is accepted by the network? Assume that there are no transactions from other (non-mining) clients, but that the miner will add transactions to reward itself. Assume the coinbase reward is 25 coins. (You may make up any transaction IDs and addresses you wish to receive the rewards).

7. (15 points) Consider the following Merkle tree:



(a) Give the Merkle path for T_B.

(b) How many hashes are needed to verify that a transaction is in a Merkle tree if the tree has N nodes?

(c) Assume all the outputs in every transaction except for T_C, T_D, and T_H are used. What is the minimum additional data that needs to be retained to verify that these transactions match with the Merkle root?

8. (5 points) Select **all** of the following true statements about DigiCash.

   A. A key feature of DigiCash's design is that the bank does not initially see the coin's globally unique ID (guid). As a result, the bank cannot tie the purchaser to any of the coins that are later redeemed with the bank.

   B. DigiCash relies on a trusted third party to serve as a central clearinghouse.

   C. DigiCash makes strong guarantees of anonymity, unless the purchaser attempts to double-spend a coin; in this case, anonymity can be broken through the use of the coin's globally unique ID (guid).

   D. Blind signatures are used to guarantee anonymity.

   E. DigiCash first invented the blockchain to establish consensus among its "miners".

9. (10 points) Answer the following questions related to mining in Bitcoin.

   (a) Bitcoin miners expend computational resources to verify transactions. Why do they bother? How are they rewarded for their efforts?

   (b) How does the network resist *Sybil attacks*, and how does mining relate to this issue?

   (c) Write pseudocode for how a miner searches for a valid proof for a given block.

10. (5 points) Select **all** of the following true statements about Bitcoin Script.

    A. Script is a stack-based, Forth-like, Turing-complete programming language, capable of creating many interesting types of transactions.

    B. Most miners only accept transactions in one of a few standard forms, though they will accept other blocks with more varied transactions.

    C. `scriptPubKey` specifies the locking script for an output; to spend the output, an input must specify a `scriptSig` unlocking script that satisfies the terms set by the locking script.

    D. *Multisignature* scripts are useful when funds should only be released when approved by multiple entities; this form can even support M-of-N signature schemes where only a specified subset of the entities needs to approve the transfer of funds.

    E. The `while` loop is the only form of looping available in Script.

11. (10 points) For a simplified DigiCash-like system, a bank receives the following coins:

```
[ { guid: 0ae7d42391, ris: [12c,382,ea1,4f2,361] },
  { guid: 4f980ec239, ris: [494,628,123,fea,7ec] },
  { guid: 989eca422f, ris: [34c,834,ff4,ef3,ec4] },
  { guid: f0e9a18341, ris: [511,f9e,cc7,ab4,00d] },
  { guid: 0ae7d42391, ris: [12c,889,5aa,4f2,86a] },
  { guid: 989eca422f, ris: [34c,834,ff4,ef3,ec4] },
  { guid: 526a4013fc, ris: [991,682,0f3,e03,697] } ]
```

    (a) Which coins indicate double spend attempts?

    (b) For each attempt you identified, was it the merchant or the coin purchaser? If the coin purchaser, reveal their identity in hex notation.

    (c) With this system, what are the odds that the coin purchaser could be responsible for a double-spend attempt, but that the merchant would appear to be at fault.

12. (10 points) Consider a simplified mnemonics setup where each word represents 3 bits. Given the seed $S = A37$ (using hex notation) and the list of words:

    - apple
    - banana
    - cherry
    - durian
    - eggplant
    - fig
    - grapefruit
    - honey

    What should the mnemonic phrase be?