Bitcoin and Blockchain

Copyright © 2019 by Wenliang Du, All rights reserved.
Personal uses are granted. Use of these problems in a class is granted only if the author's book is adopted as a textbook of the class. All other uses must seek consent from the author.

C6.1. Why did Bitcoin use an elliptic-curve-based public-key algorithm, instead of using the popular RSA algorithm?

C6.2. What is the length of the publish key hash in the Bitcoin system?

C6.3. Please identify the type (a public-key hash or a script hash) of a bitcoin address if (1) the first character of the Base58-encoded Bitcoin address is '1', or (2) the first character of the Base58-encoded Bitcoin address is '3'?

C6.4. Bob got 5 bitcoins from Alice, and he pays Charlie 3 bitcoins in a transaction. What happens to the leftover (2 bitcoins)?

C6.5. Alice got 5 Bitcoins from a previous transaction, and she wants to use these 5 Bitcoins to pay Bob 2 Bitcoins and pay Charlie 2.99 Bitcoins. She wants to create two different transactions for these purposes. Is this doable?

C6.6. A transaction is locked using the following script. (1) Please provide the corresponding unlocking script. (2) Is this locking script secure?

```
<3> OP_MUL OP_ADD <50> OP_EQUAL
```

C6.7. The output of a transaction is locked using the followings standard pay-to-pubkey-hash script. (1) Who can provide a valid unlocking script? (2) An attacker wants to spend the money included in this locked output. After seeing the valid unlocking script, the attacker immediately copies the unlocking script to his own transaction. Does this work?

```
scriptPubKey: OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY
              OP_CHECKSIG
scriptSig:    <sig> <pubKey>
```

C6.8. In pay-to-pubkey-hash transactions, an output from a previous transaction T is used as one of the inputs. To unlock this output, a signature must be provided. Bob's understanding is that the signature is generated from the transaction T, not from the current transaction. If what Bob says is true, is it secure?

C6.9. Bob got 3 bitcoins from a pay-to-script-hash transaction. To spend the money in his transaction, he needs to provide a unlocking script, which contains a redeem script. Unfortunately, when he types the redeem script, he made a mistake. What is going to happen?

C6.10. To receive a payment from Alice, Bob gave Alice one of his public keys, and Alice paid 3 bitcoins to this public key. Later, Bob realized that he has given Alice the wrong key: the key he gave to Alice is a "dead" key because he has lost its matching private key. Can Bob ask Alice to void the transaction? What is going to happen to the bitcoins in this payment?

C6.11. When a miner sees two branches in a blockchain, which branch should be accepted?

C6.12. What is the confirmation number?

C6.13. What are the incentives for Bitcoin miners?

C6.14. Bob finds an efficient way to solve the following problem: For any hash function, given a number h and two strings $M1$ and $M2$, find a number R, such that $\texttt{hash}(M1 \| R \| M2) = h$. What is the impact of this discovery on the Bitcoin system.