Assignment 02

The due date for submitting this assignment has passed. **Due on 2020-03-11, 23:59 IST.**

Score: 9/10=90%

Assignment submitted on 2020-03-11, 14:14 IST

1) In public key cryptosystem based digital signature, the message digest is signed by: ***1 point***

- (•) sender's private key
- ( ) sender's public key
- ( ) receiver's private key
- ( ) receiver's public key

Yes, the answer is correct.
Score: 1
Accepted Answers:
sender's private key

2) In crypto-currency a ledger records? ***1 point***

- ( ) list of balances
- (•) list of transactions
- ( ) list of accounts
- ( ) none of the above

Yes, the answer is correct.
Score: 1
Accepted Answers:
list of transactions

3) a. What defines a valid ledger? ***1 point***
b. Given a valid ledger can you generate account balances?

- ( ) a. All transaction are valid
  b. No

a. All transaction are valid
b. yes

a. some transaction can be invalid
b. No

a. some transaction can be invalid
b. yes

Yes, the answer is correct.
Score: 1
Accepted Answers:
a. All transaction are valid
b. yes

4) Repudiation/ verifiability problem can be solved by digitally signing transaction by sender in Blockchain? ***1 point***

false
true

Yes, the answer is correct.
Score: 1
Accepted Answers:
true

5) When will replay attack happen? ***1 point***

a. Sender Account balance after transaction is greater than or equal to the amount transferred in the transaction.
b. "Change Address" is included in the transaction
c. Sender Account balance after transaction is less than the amount transferred in the transaction.

a. Yes
b. No
c. Yes

a. No
b. Yes
c. No

a. Yes
b. Yes
c. Yes

a. Yes
b. No
c. No

Yes, the answer is correct.
Score: 1

Accepted Answers:
a. Yes
b. No
c. No

6) Fischer-Lynch-Paterson impossibility result: consensus is impossible with even a single faulty node? **1 point**

false
true

Yes, the answer is correct.
Score: 1

Accepted Answers:
true

7) Which of the following is/are decentralised system? **1 point**

DNS
Bitcoin
SMTP
None of the above

No, the answer is incorrect.
Score: 0

Accepted Answers:

Bitcoin

8) Why consensus is hard? **1 point**

- [x] No notion of global time
- [x] faults in network
- [x] nodes may crash/ faulty nodes
- [ ] none of the above

Yes, the answer is correct.
Score: 1

Accepted Answers:

No notion of global time

faults in network

nodes may crash/ faulty nodes

9) Paxos is? **1 point**

- [x] Consistent
- [ ] Inconsistent
- [x] rarely stuck
- [ ] never stuck

Yes, the answer is correct.
Score: 1

Accepted Answers:

Consistent

rarely stuck

10) Is Byzantine General Problem solvable for 3 nodes? **1 point**

- (•) false
- ( ) true

Yes, the answer is correct.
Score: 1