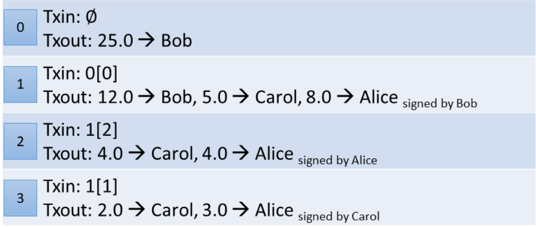
Exercise 3

A. Transactions

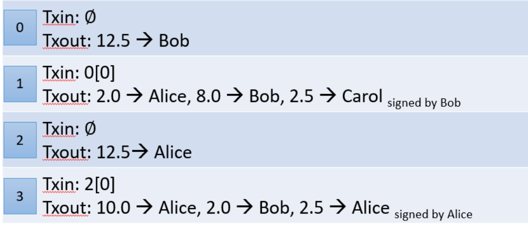
1. Consider the following transactions in a transaction based ledger. Check if the transactions are valid. If valid calculate the balances of each person.

(a)



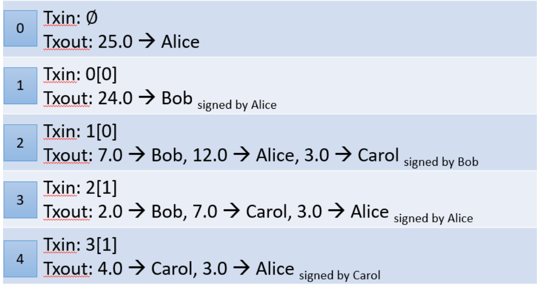
0	Txin: Ø Txout: 25.0 → Bob
1	Txin: 0[0] Txout: 12.0 → Bob, 5.0 → Carol, 8.0 → Alice signed by Bob
2	Txin: 1[2] Txout: 4.0 → Carol, 4.0 → Alice signed by Alice
3	Txin: 1[1] Txout: 2.0 → Carol, 3.0 → Alice signed by Carol

(b)



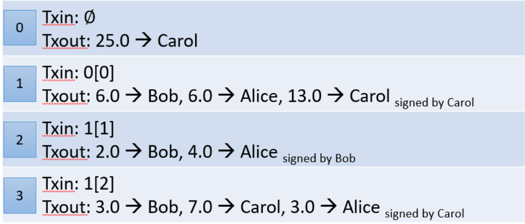
0	Txin: Ø Txout: 12.5 → Bob
1	Txin: 0[0] Txout: 2.0 → Alice, 8.0 → Bob, 2.5 → Carol signed by Bob
2	Txin: Ø Txout: 12.5→ Alice
3	Txin: 2[0] Txout: 10.0 → Alice, 2.0 → Bob, 2.5 → Alice signed by Alice

(c)



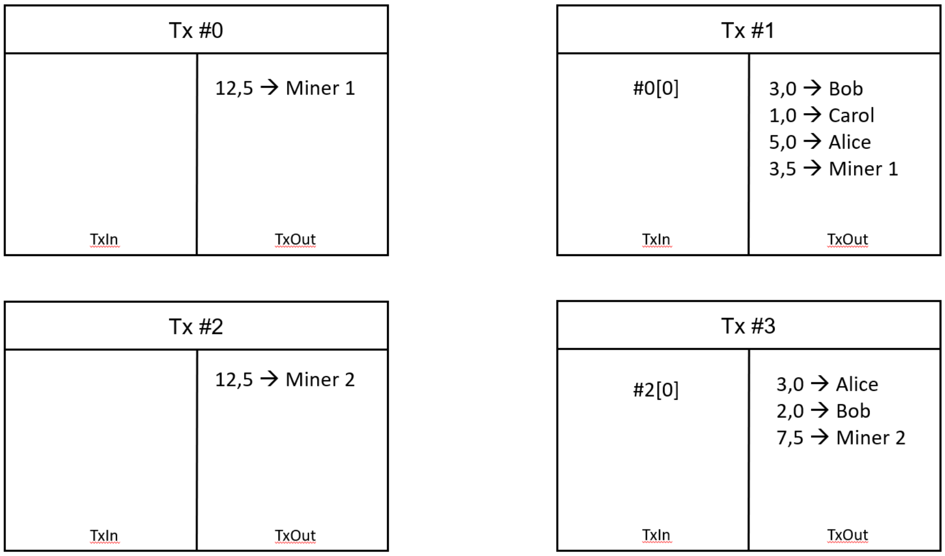
0	Txin: Ø Txout: 25.0 → Alice
1	Txin: 0[0] Txout: 24.0 → Bob signed by Alice
2	Txin: 1[0] Txout: 7.0 → Bob, 12.0 → Alice, 3.0 → Carol signed by Bob
3	Txin: 2[1] Txout: 2.0 → Bob, 7.0 → Carol, 3.0 → Alice signed by Alice
4	Txin: 3[1] Txout: 4.0 → Carol, 3.0 → Alice signed by Carol

(d)



0	Txin: Ø Txout: 25.0 → Carol
1	Txin: 0[0] Txout: 6.0 → Bob, 6.0 → Alice, 13.0 → Carol signed by Carol
2	Txin: 1[1] Txout: 2.0 → Bob, 4.0 → Alice signed by Bob
3	Txin: 1[2] Txout: 3.0 → Bob, 7.0 → Carol, 3.0 → Alice signed by Carol

2. Below is the representation of four transactions in the Bitcoin network where Alice receives Bitcoins from two different miners. Transaction fees are ignored.



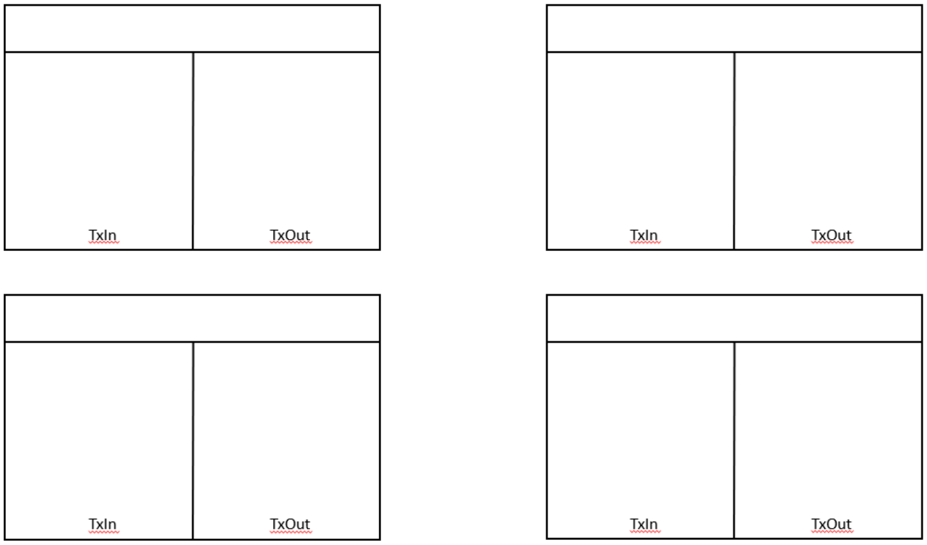
Tx #0	
	12,5 → Miner 1
TxIn	TxOut

Tx #1	
#0[0]	3,0 → Bob 1,0 → Carol 5,0 → Alice 3,5 → Miner 1
TxIn	TxOut

Tx #2	
	12,5 → Miner 2
TxIn	TxOut

Tx #3	
#2[0]	3,0 → Alice 2,0 → Bob 7,5 → Miner 2
TxIn	TxOut

Alice now wants to make two payments. She wants to transfer Carol 6,0 BTC and Bob 0,5 BTC. Draw the necessary transactions for Alice using the notation of diagram above.



3. Bitcoin clients and exchanges provide ”block explorers” that let users search transactions, blocks, addresses and other relevant blockchain network information. One of the well-known Bitcoin block explorer is `https://www.blockchain.com/explorer`.

   Visit the block explorer and find the following information for the Bitcon blockchain:

   (a) What is the current hash rate?

   (b) What was the all time peak value of unconfirmed transactions and when has it occured?

   (c) Find the transaction a1075db55d416d3ca199f55b6084e2115b9345e16c5cf302fc80e9d5fbf5d48d. Fill the following information:

      (a) Block of the transaction

      (b) Sender and the receiver

(c) The value of the transaction

(d) What is particular about this transaction?

B. Bitcoin Script

4. Take a look at Bitcoin script's opcodes in the slides. Which fundamental commands are missing? What could be the reason they are not added?

5. Alice wants to protect her Bitcoins and therefore her unspent transaction outputs. She decides to protect it with a password. She hashes the password and writes a script: The script requires the person (which intends to spend the output) to provide the password as an input. This input is hashed and compared to the predefined hash, proving that Alice spends the transaction. What are the possible flaws with this Bitcoin Script?

6. There is an op_code called locktimeverify and a time lock in the transaction itself. What is the difference? What are examples in which these are useful?

7. Following transaction output is provided:

```
OP_DUP OP_HASH160 8a014218a5a42e2c6fc5d573ab54a91ff555d1de OP_EQUALVERIFY OP_CHECKSIG
```

   (a) Can you tell which entity has created this transaction output?

   (b) Can you tell if this transaction output is spent?

   (c) Can you tell which entity is allowed to spend this transaction output?

   (d) What specific data is required to spend the transaction output?