Bitcoin Basics

A. Bitcoin Network and Storage

1. Explain the function of the memory pool in the Bitcoin network.

2. We have two investors Alice and Bob. Alice is day trading Bitcoin as a hobby and Bob has bought some Bitcoin as part of his children's college funds. For each of them, argue whether they should use a hot or cold wallet and suggest a specific wallet as an example.

B. Transactions

3. 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

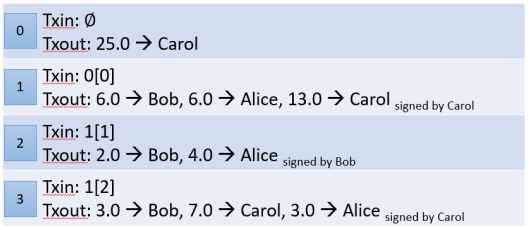
(b)

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

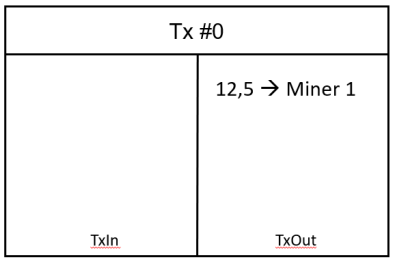
(c)

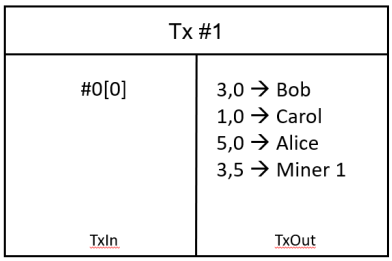
0	Txin: Ø Txout: 25.0 → Alice
1	Txin: 0[0] Txout: 24.0 → Bob signed by Alice
2	Txin: 1[0] Txout: 7.0 → Bob, 12.0 → Alice, 3.0 → Carol signed by Bob
3	Txin: 2[1] Txout: 2.0 → Bob, 7.0 → Carol, 3.0 → Alice signed by Alice
4	Txin: 3[1] Txout: 4.0 → Carol, 3.0 → Alice signed by Carol

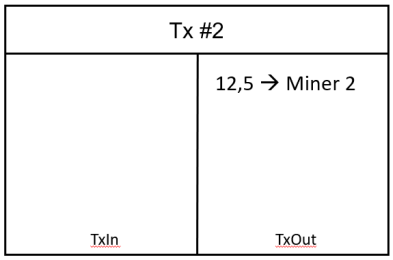
(d)

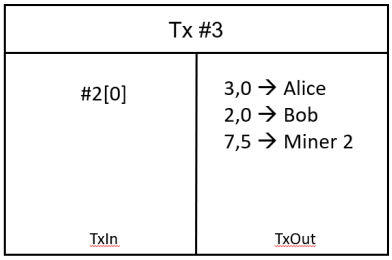

0
Txin: Ø
Txout: 25.0 → Carol
1
Txin: 0[0]
Txout: 6.0 → Bob, 6.0 → Alice, 13.0 → Carol signed by Carol
2
Txin: 1[1]
Txout: 2.0 → Bob, 4.0 → Alice signed by Bob
3
Txin: 1[2]
Txout: 3.0 → Bob, 7.0 → Carol, 3.0 → Alice signed by Carol

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

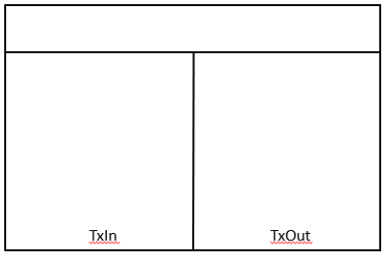


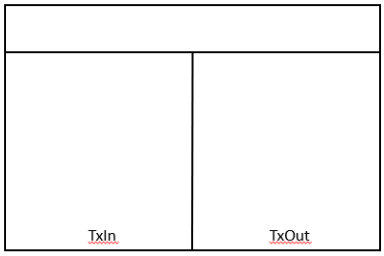


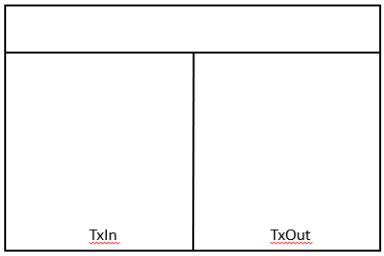


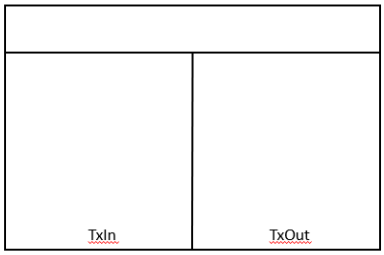


Alice now wants to make two payments. She wants to transfer Carol 6,0 BTC and Bob 0,5 BTC. Draw the necessary transactions for Alice using the notation of diagram above.









5. Bitcoin clients and exchanges provide "block explorers" that allow users search transactions, blocks, addresses and other relevant blockchain network information. One of the well-known Bitcoin block explorer is https://blockchair.com/bitcoin/.

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

   (a) What is the current hash rate?

   (b) What was the all time peak value of unconfirmed transactions and when has it occured? You might also take a look here: https://www.blockchain.com/explorer

   (c) There is no objectively correct number to the previous question. Explain why.

   (d) 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?