Bitcoin Basics

A. Bitcoin Network and Storage

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

> **Solution:**
>
> The memory pool stores all transactions which are not contained in a block yet. Each full node maintains the list of these transactions and updates it when 1) a new block arrives and 2) new transactions arrive.

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.

> **Solution:**
>
> - Alice should be using a hot wallet: As Alice is day trading Bitcoins, her Bitcoins should be available at any time for easy access and use. So a wallet that is connected to internet is the suitable option for her where Bitcoins are delivered directly to the wallets through fast online transactions. Alice could use online hot wallets like the ones available in Coinbase or Binance.
> - Bob should be using a cold wallet: Bob's main concern is the secure storage of Bitcoins and not the easy use or access to them. He could use a hardware wallet such as Trezor or a paper wallet.

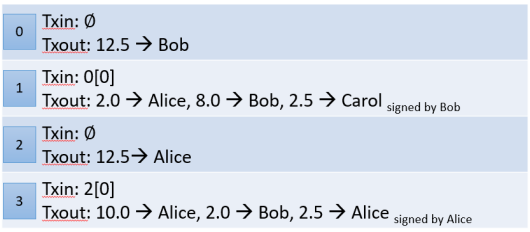
B. Transactions

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)

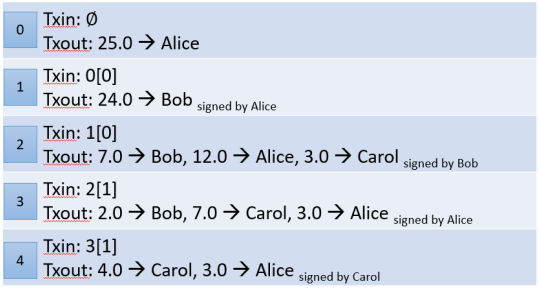
Solution:
Transactions are valid
Alice = 7.0 Bob = 12.0 Carol = 6.0

(b)



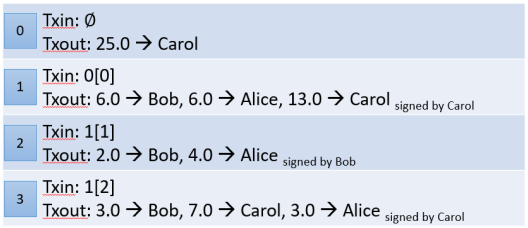
Solution:
Transactions are not valid. At Tx3 the Txin 2[0] has 12.5 coins whereas the Txouts sum up to 14.5 coins. Even though Alice has a balance of 14.5 coins Tx3 is not valid as $\sum Txin < \sum Txout$. To make the transaction correct, Tx3 would not only have to use Txin 2[0], but also Tx1[0].

(c)



Solution:
Transactions are valid
Alice = 6.0 Bob = 9.0 Carol = 7.0
In this case at Tx1 Alice, and at Tx2 Bob both do not redeem the full amount remaining from the respective Txin. Those balances can be claimed by miners as a transaction fee.

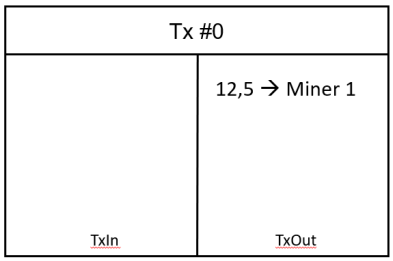
(d)

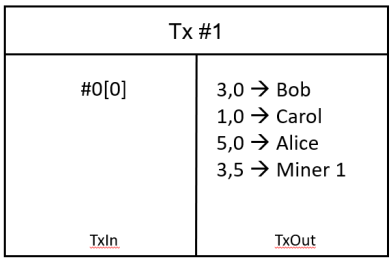


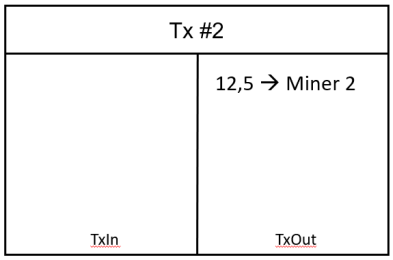
Solution:

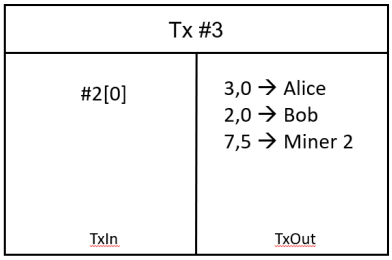
Transactions are not valid. At Tx2 the Txin 1[1] is owned by Alice. Therefore Bob cannot use this Txout for his transaction. He would have to use Txin 1[0].

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

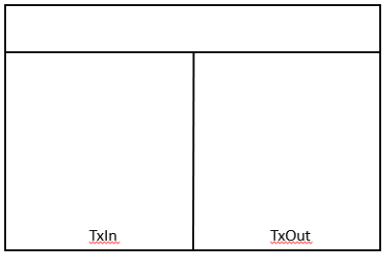


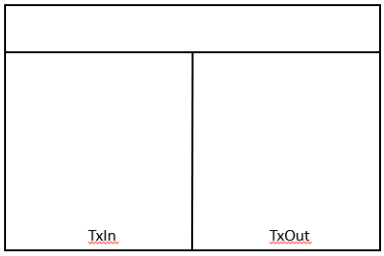


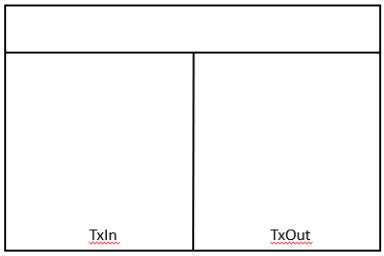


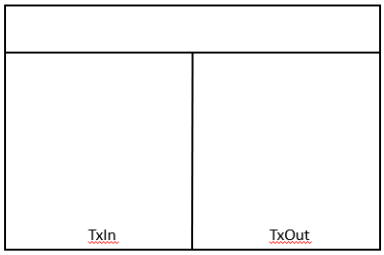


Alice now wants to make two payments. She wants to transfer Carol 6,0 BTC and Bob 0,5 BTC. Draw the necessary transactions for Alice using the notation of diagram above.

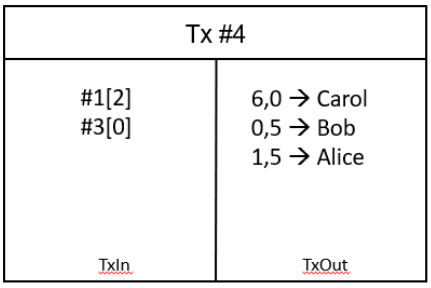








Solution:



Different combinations of transactions are also possible, such as sending first to Carol and then to Bob. In the context of our exercise, it is okay to create two or three transactions. Please note: It could be possible that we ask about the "solution with the minimum amount of transactions", which would result in the above presented solution as the only correct one.

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?

   Solution:
   Current hash rate is around 220.76 Eh/s (18.05.2022)

   (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

   Solution:
   The peak value is 178,640 transactions unconfirmed at 19.05.2017.

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

   Solution:
   There is no "objectively correct" number to the highest amount of unconfirmed transactions in the network, as different nodes have a different perception of the network. E.g., https://jochen-hoenicke.de/queue report a higher number of unconfirmed transactions in the mempool on December 22, 2017 with a peak value of roughly 261,000 transactions.

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

(a) Block of the transaction:

Solution:
Block number 57043.

(b) Sender and the receiver:

Solution:
Sender: 1XPTgDRhN8RFnzniWCddobD9iKZatrvH4
Receiver: 17SkEw2md5avVNyYgj6RiXuQKNwkXaxFyQ

(c) The value of the transaction:

Solution:
10,000 Bitcoins (plus 0.99 BTC fee)

(d) What is particular about this transaction?

Solution:
This transaction was sent from a https://bitcointalk.org/index.php?topic=137.msg1195user in 2010 for a pizza. At that time it was worth around 25$. Please note that Blockchain.com website displays the US$value based on the current price of Bitcoin.