Bitcoin Basics

Bitcoin Network and Storage

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

> The memory pool stores all transactions which are not contained in a block yet (i.e., not confirmed). 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, argue whether they should use a hot or cold wallet and suggest a specific wallet as an example.

> - 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 Ledger, or a paper wallet.

3. Payment channels such as Lightning Network on Bitcoin are known as Layer-2 (L2) solutions. Briefly explain why these solutions are called L2, and list two potential drawbacks.

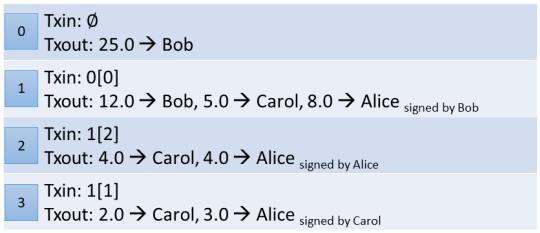
> Payment channels, e.g., Lightning Network (LN), are also known as Layer-2 (L2) solutions as they operate not directly inside the underlying base (Layer-1) network but on their own, separate network, which is built on top of the L1 network. L2 solutions scale the underlying L1 by:
>
> - processing transactions on their own network, which has a much higher throughput (e.g., 7 tx/s on Bitcoin vs. 1,000,000 tx/s on LN), and
> - only publishing minimal-required information on the L1 (e.g., open channel, close channel settlement transactions).
>
> Using L2s, users avoid paying high transaction fees and waiting long block times (Bitcoin - 10 minutes). However, L2s or, more specifically, payment channels, as there are different L2 solutions available, have their drawbacks:
>
> - By processing transactions off-chain, payment channels significantly limit the transparency/traceability/auditability features of the underlying L1.

- Transactions on the L2 are no more L1 (e.g., Bitcoin) transactions. Hence, the security measures of the L1 do not protect user transactions anymore. This could introduce regulatory problems for the L2 maintainers.
- Bitcoin's Lightning Network (LN) enables users to transact with each other even when they don't have a channel opened between them. For example, let's assume Alice wants to send Bitcoins to Carol, but Alice and Carol don't have a channel in-between. However, Bob (a friend of Alice and Carol) has channels with both of them. In this case, Alice can route her transaction to Carol through Bob. You can read more about LN transactions **here**.
  Finding the optimal route when there are only three users and two channels is trivial. However, LN currently has over 12k nodes and 50k channels, which constantly update (more stats are available on `https://mempool.space/lightning`). Hence, finding an optimal route on a dynamically changing network topology is a **hard problem**. This results in payment failures on LN as the protocol fails to find a route.

Transaction-based Ledger

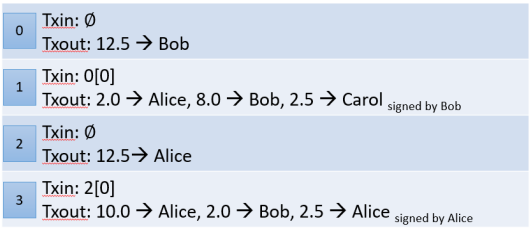
1. Consider the following transactions in a transaction-based ledger like Bitcoin. Check if the transactions are valid. If valid, calculate the balance of each person.

(a)



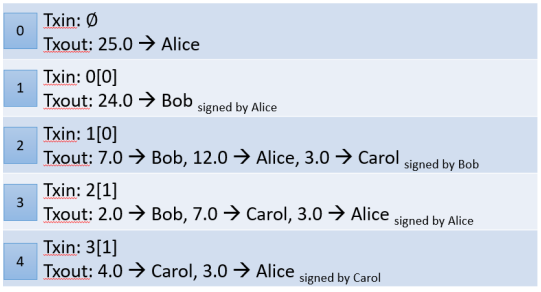
Transactions are valid
Alice = 7.0 Bob = 12.0 Carol = 6.0

(b)



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)



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)

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

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].

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

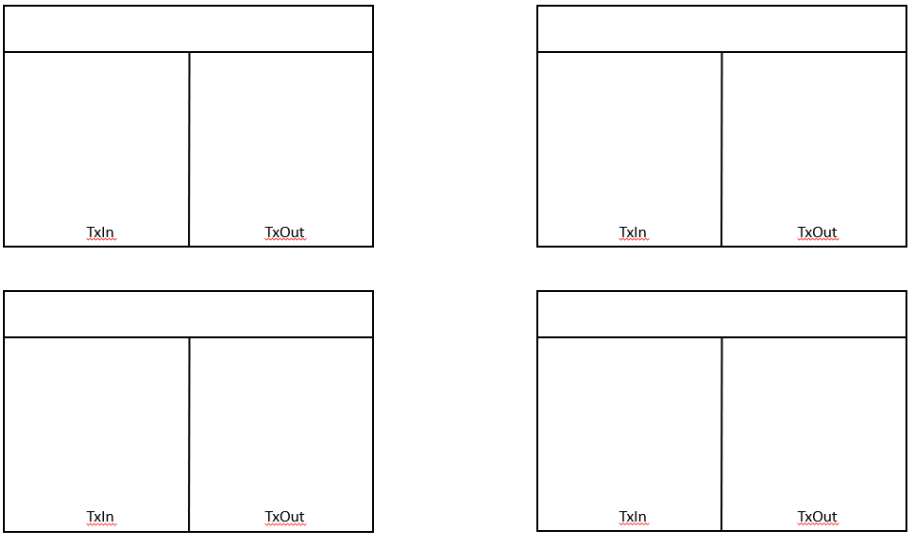
Tx #0	
TxIn	12,5 → Miner 1 TxOut

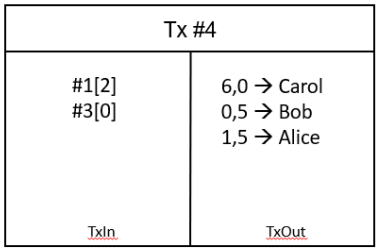
Tx #1	
#0[0] TxIn	3,0 → Bob 1,0 → Carol 5,0 → Alice 3,5 → Miner 1 TxOut

Tx #2	
TxIn	12,5 → Miner 2 TxOut

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





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.

3. Bitcoin clients and exchanges provide "block explorers" that allow users to search transactions, blocks, addresses, and other relevant blockchain network information. One of the well-known Bitcoin block explorers 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?

   > Current hash rate is around 606.26Eh/s (20.04.2024)

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

   > The peak value is 316,090 unconfirmed transactions, observed on 12.08.2023.

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

   > 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 05.09.2023, with a peak value of roughly 610,404 transactions.

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

      i. Block of the transaction:

      > Block number 57043.

      ii. Sender and the receiver:

      > Sender: 1XPTgDRhN8RFnzniWCddobD9iKZatrvH4
      > Receiver: 17SkEw2md5avVNyYgj6RiXuQKNwkXaxFyQ

iii. The value of the transaction:

> 10,000 Bitcoins (plus 0.99 BTC fee)

iv. What is particular about this transaction?

> This transaction was sent from a user in 2010 for a pizza. At that time it was worth around $41. Please note that Blockchain.com website displays the $ value based on the current price of Bitcoin.