Homework 4

Alice has an idea for a startup. She wants to run a service to help people buy and sell concert tickets on the Ethereum blockchain. Her idea is revolutionary because it uses atomic swaps to eliminate the need for trusted intermediaries, cutting out all the fees added by payment processors, brokers, and other middle-men. Alice's company can take a small commission on each sale, and still dramatically undercut the competition. Her protocol works as follows:

- Let's say Bob wants to buy a ticket and Carol wants to sell a ticket. The sale price of the ticket is 1 Eth, and Alice takes a 5% commission. The ticket is represented as an ERC721 token.
- Bob, Carol and Alice each generate a secret off-chain and hash it to create a hashlock that can only be unlocked by producing the secret that generated it.
- Bob and Carol then send off-chain messages to Alice saying that they want to buy / sell a ticket to the concert. These messages include their hashlocks.
- Alice sees both requests and pairs them together. She then sends replies to both parties that include Alice's own hashlock and the hashlock of the remaining party so that everyone has all 3 hashlocks. Alice also instructs Bob and Carol to escrow their respective assets on the Ethereum blockchain by sending them to special escrow contracts written by Alice's company.
- Once everything's in escrow, Bob and Carol generate signed transaction components off-chain.
  - Transaction components are structs that specify a transfer amount, sender and recipient. They also contain the 3 hashlocks and a signature produced by taking the above data and hashing it with the sender's Ethereum private key. This signature allows the escrow contract to verify that the transaction component was produced by the sender.
  - When a signed transaction component is published to an escrow contract along with the 3 secrets that unlock the hashlocks, the escrow contract modifies the balances of each participant according to the instructions in the transaction component. Without all 3 secrets, publishing a transaction component does nothing (reverts).
- Bob generates 2 transaction components. Let's call these TX1 and TX2.
  - TX1 transfers .95 Eth from Bob to Carol.
  - TX2 transfers .05 Eth from Bob to Alice. This is Alice's 5% commission.
- Carol generates 1 transaction component, TX3.
  - TX3 transfers 1 ticket from Carol to Bob.
- Bob sends TX1 and TX2 to Carol and Alice, respectively. Carol sends TX3 to Bob. These messages are sent off-chain.
- Now that Bob and Carol have received their transaction components, they know they can claim their intended assets as soon as they have everyone's secrets. Furthermore, they know that no one can publish a transaction component without publishing all 3 secrets to the public blockchain. Feeling good about all this, Bob and Carol send Alice the secrets to unlock their hashlocks.
- At this point, Alice is the only one who knows all 3 secrets. However, she cannot steal Bob’s Eth because (as mentioned above) if she publishes her transaction component she must also publish the 3 secrets to the blockchain. Once she does this, Bob and Carol will also have all 3 secrets and will publish their transaction components as well, completing the transaction as intended.
- Finally, escrow contracts unlock after a specified timeout 𝑇, allowing anyone to withdraw whatever balance is recorded for them in the contract. We assume off-chain messages are sent in negligible time and that publishing a transaction component takes a fixed time 𝛿.
Questions:

1. Suppose that instead of using a timeout, the escrow contracts only unlock once they receive a signed transaction component and all 3 secrets. Explain why this version of the protocol is not atomic.

2. How long (in terms of Δ) after funds are escrowed should we make the timeout T in order to ensure the protocol is atomic? If no such timeout exists, please explain why.

For the following 2 questions, assume Alice is completely trustworthy and always conforms to the protocol. After all, her business depends on it. Furthermore, let’s adjust the protocol so that once Alice has all 3 secrets, she immediately shares them with both Bob and Carol. That way, Bob and Carol are guaranteed the ability to claim their intended assets provided they both share their secrets with Alice.

3. Under these new assumptions, the protocol can function similar to off-chain payment channels like the lightning network. Timeouts can be set far in the future, and many micro transactions can occur between Bob and Carol off-chain before they are settled on-chain. However, participants would have to store a record of every transaction component to ensure they all get published to the blockchain before the timeout. Furthermore, sending so much data to the blockchain at once could have an extremely high gas cost. What fields could be added to the transaction component structs so that only the most recent one needs to be sent to each escrow contract for settlement?

4. Is the protocol atomic if we assume Alice never deviates from it? Explain why or why not. (Hint: Consider what the digraph of this swap looks like.)