Cryptocurrencies (WS 2021) Univ-Prof. Dr. Matteo Maffei

Retake Exam: Part B

Date: 24/02/2022 TU Wien

Name: ***Matriculation Number:***

- You should be alone and keep your camera switched on during the exam.
- Part B of the exam takes 90 minutes. You can get at most 30 points. The number of points you can get for an exercise thus gives you a hint about how much time you should spend on that exercise.
- **Write legibly and be concise**. It is in your best interest that we understand your answers. You will be graded not only on the correctness of your answer, but also on the clarity with which you express it.
- When finished, the solution should be uploaded back in TUWEL in the form of a PDF file as well. You can use dedicated apps (e.g., Adobe Scan, MS Office Lens), print and scan, or whichever solution you find more convenient.
- Good luck!

Problem	1	2	**Total**
Score			
Points	10	20	

Name:	/ Matriculation Number:

Problem 1: Blockchain Usage (10 points)

In this exercise we assume the standard consensus and mining strategies from Bitcoin, but simplify the underlying data structure:

- Every block contains only a single transaction.
- Transactions are of the form $\langle id, id', \mathsf{pk}_R \rangle_{\mathsf{sk}_S}$, where
  - id is the transaction's unique identifier;
  - id' is the identifier of the transaction that is spent;
  - pk_R is the address of the receiver of the payment;
  - sk_S is the secret key of the sender used for signing the transaction.
- Every transaction transfers exactly one coin.
- A block is of the form $[\![nonce, p, t]\!]$, where $nonce$ is the nonce for the proof of work, p is the hash pointer to the previous block and t is the transaction.
- For appending a block $[\![nonce, p, \langle id, id', \mathsf{pk}_R \rangle_{\mathsf{sk}_S}]\!]$ to the blockchain, it needs to hold that
  - p is the hash of a block b in the chain ;
  - $H(nonce||p||\langle id, id', \mathsf{pk}_R \rangle_{\mathsf{sk}_S}) < target$, for some fixed target $target$, holds (a proof of work as in Bitcoin is used);
  - The chain starting from b contains a transaction with identifier id' and receiver pk_S, but this transaction was not spent by another transaction in the chain.
- As in Bitcoin, honest miners always mine on the longest chain (this does not necessarily mean that they always append to the longest chain, due to the concurrency of the system).

Assume that Alice (with private key sk_A and public key pk_A), Bob (with private key sk_B and public key pk_B), and Charlie (with private key sk_C and public key pk_C) are three users of the Bitcoin network. We start with an initial blockchain of the following form:

where $[\![nonce_1, \bot, \langle 1, \bot, \mathsf{pk}_C \rangle_{\mathsf{sk}_c}]\!]$ denotes the (singular) genesis block that does not have a predecessor (denoted by $\bot$), and is not spending an existing transaction, but creates a new one (denoted by referencing transaction $\bot$).

Now Alice wants to buy a good G from Bob for one coin. To do so, they perform the following protocol:

1. Alice submits a transaction $t = \langle 3, 2, \mathsf{pk}_B \rangle_{\mathsf{sk}_A}$ to the network.
2. As soon as the (valid) block $[\![nonce, H(b), t]\!]$ is appended to the blockchain for some block b, Bob sends G to Alice.

Exercises

1. **(5 points)** Give a potential attack that shows how Alice can receive G without spending her coin to Bob. To this end, you should give a sequence of blocks that can be appended to the blockchain by honest miners such that the conditions for Bob are satisfied at some point in this sequence to send G to Alice, but that at the end of the sequence according to the longest chain, Alice did not lose any coins. Sketch the intermediate states of the blockchain after each block, argue why appending the block in the described fashion is fine, and mark the point where Bob sends G to Alice.
2. **(5 points)** Assume that Bob waits for 6 blocks to follow Alice's payment transaction before sending G to Alice. Is the described protocol secure if more than 50% of the hash computation power is contributed by honest miners? Does this change if Alice contributes more than 50% of the the system's computation power? If not, argue why, if yes, show an attack where Bob sends G to Alice and Alice does not lose any coins.

Name:	/ Matriculation Number:

Space for your answer

Name:	/ Matriculation Number:

Extra space

Name:	/ Matriculation Number:

Problem 2: Discreet Log Contracts (20 points)

A Discreet Log Contract (DLC) allows two untrusted users to bet on the outcome of a certain event. For setting up a DLC, we need to consider 3 parties: Alice, Bob and Oscar. Alice and Bob bet on whether Alice will pass or fail the Cryptocurrencies exam. They lock up 1 BTC each and if Alice passes the exam she will get 2 BTC, otherwise, if she fails Bob will get all the coins. Oscar is a trusted oracle that will publish Alice's result: he publishes 1 if Alice passes, and 0 if she fails. In DLCs there are two constructions that play a crucial role: the modified Schnorr signature scheme and the Contract Execution Transactions (CETs).

Schnorr Signature. Alice and Bob respectively sample private scalars, a and b. They compute their public keys $pk_A = aG$ and $pk_B = bG$, where G is the publicly known group generator. To create a signature s, each party first needs to sample a random private scalar k and compute $R = kG$. Let H be a hash function.[1] The signatures are constructed as follows:

$$(s_{A,m}, R_A), \quad \text{Alice's signature over the message } m, \text{ where } s_{A,m} = k_A - H(m, R_A)a$$
$$(s_{B,m}, R_B), \quad \text{Bob's signature over the message } m, \text{ where } s_{B,m} = k_B - H(m, R_B)b$$

Given (pk_A, m, R_A, s_A), Bob can check the validity of Alice's signature over m if the following relation holds:

$$s_{A,m}G = R_A - H(m, R_A)pk_A = k_AG - H(m, R_A)aG$$

In an analogous way, Alice can check Bob's signature over m.

Schnorr for DLC. The public key is now given by (pk, R) and a signature over a message m is s_m alone. Notice that with this new construction, Oscar discloses his public key $(pk_O = oG, R_O = k_OG)$. Since R_O is publicly known, before any signature $s_{O,m}$ is computed by Oscar, anyone is able to compute $s_{O,m}G$ for any m:

$$s_{O,m}G = R_O - H(m, R_O)pk_O$$

Contract Execution Transactions. With Contract Execution Transactions we refer to $\{m\} \times \{P\} = \{0, 1\} \times \{\text{Alice, Bob}\}$ transactions: we have two possible outcomes from the oracle, i.e., either 1 or 0, and two parties involved in the bet, namely Alice and Bob. This results in two transactions held by Alice and two transactions held by Bob for each of the outcomes, so that each party can unilaterally close the bet at the correct state. All the CETs spend from the same output and have the following logic for their output scripts:

$$pk_{A,m} \text{ OR } (pk_B \text{ AND TimeDelay}), \quad \text{transactions held by Alice}$$
$$pk_{B,m} \text{ OR } (pk_A \text{ AND TimeDelay}), \quad \text{transactions held by Bob}$$

where

$$pk_{A,m} = pk_A + s_{O,m}G = aG + R_O - H(m, R)pk_O$$
$$pk_{B,m} = pk_B + s_{O,m}G = bG + R_O - H(m, R)pk_O$$

When Oscar reveals his signature $s_{O,m} = k_O - h(m, R_O)o$ over message m, Alice and Bob can compute their respective secret keys $sk_{A,m}$ and $sk_{B,m}$, which allow them to claim the funds corresponding to the outcome of the bet. The secret keys $sk_{A,m}$ and $sk_{B,m}$ for $pk_{A,m}$ and $pk_{B,m}$ are as follows:

$$sk_{A,m} = sk_A + s_{O,m} = a + s_{O,m}$$
$$sk_{B,m} = sk_B + s_{O,m} = b + s_{O,m}$$

Exercises

1. **(15 points)** Given that DLCs operate similar to the constructions we have seen for the payment channel networks (e.g., Lightning Network), describe how the DLC works. Namely, describe on a conceptual level: (i) how the funding transaction will look like; (ii) how the CETs will look like and over which transactions Alice and Bob exchange signatures; (iii) how the funds will be redeemed.

[1] Note that with $H(a, b)$ we denote applying the hash function on the string concatenation of a and b.

2. **(5 points)** Assume that Alice publishes the execution transaction in advance, when Oscar has not yet published the exam result (Passed/Failed). Is she able to spend the output of the execution transaction? If yes, describe under which conditions and elaborate on the different possibilities.

Space for your answer

Name:	/ Matriculation Number:

Extra space