CS251: Cryptocurrencies and Blockchain Technologies **Fall 2018**

Assignment #2

Due: 11:59pm on Mon., **Oct. 22, 2018**
Submit via Gradescope (each answer on a separate page) code: **9RZGVZ**

Problem 1. Suppose two groups independently implement the Bitcoin protocol. Some miners run implementation A and other miners run implementation B. At some point an attacker finds a vulnerability in implementation A that causes miners running that implementation to accept transactions that double spend a UTXO. Implementation B treats such transactions as invalid.

a. Suppose 80% of the mining power runs the buggy implementation and 20% runs the non-buggy one. What will happen to the blockchain once a block containing a double-spending transaction is submitted to the network?

b. What will happen to the blockchain in the reverse situation where 20% of the mining power runs the buggy implementation and 80% runs the non-buggy one?

Problem 2. A multi-judge escrow service. In lecture 6 we saw how to use a 2-out-of-3 multisig address to build an escrow service where Alice can buy a product from Bob and, if all goes well, Alice gets the product and Bob gets paid. Otherwise a judge can adjudicate the dispute. One issue with that protocol is that the judge may demand a service fee and the participants, Alice and Bob, have no choice but to pay. In this question your goal is to design an escrow system where, ahead of time, Alice and Bob agree on the set of three judges so that during adjudication they can choose any one of the three to adjudicate. We are assuming that the three judges are honest and consistent so that all three will always rule the same way.

Show how to implement a three-judge escrow system using a single *standard* multisig transaction to a multisig address that Alice and Bob agree on ahead of me. Your design must ensure that even if the three judges collude, they cannot steal the funds that Alice sends to Bob. Recall that if all goes well then the parties need not involve the judges. If something goes wrong, then any one of the three judges can adjudicate.
Hint: You will need to use a t-out-of-n multisig address where $n > 5$. Alice and Bob will be given more than one secret key each.

Problem 3. Let's go back to the basic escrow scheme from lecture 6 where there is only a single judge. A web store decides to accept Bitcoin payments using this escrow scheme from lecture 6. Specifically, the buyer sends the exact price she is paying to a 2-out-of-3 multisig address in which the buyer, web store, and judge each have one of the three keys. If either party refuses to release the funds, the other party contacts the judge who releases 95% of the funds (keeping a 5% fee for the arbitration services).

a. The web store finds that a large fraction of users never bother releasing the funds after receiving goods in the mail. Hence, the store suffers delayed payments and lost revenue to arbitration fees. How might the store incentivize buyers to release funds when they receive their goods?

b. The store's competitor writes a whole bunch of fake negative Yelp reviews accusing the store of "selling" inventory they don't actually have, and therefore costing customers the 5% arbitration fee. How can the web store convince customers to ignore these fake complaints?

Problem 4. In this exercise we look at two estimates for the amount of energy consumed by the Bitcoin network. Assume in your answer that the current exchange rate is 1BTC = US$6000 and that there are no transaction fees (only the block reward of 12.5BTC per block). Recall that energy is measured in killoWatt-hours (kWH). You may assume that one bitcoin block is generated every 10 minutes exactly.

a. Estimate the network's hourly energy consumption assuming the entire block reward is spent on electricity for mining. Use US$0.05/kWH as the price of energy and express your answer in kWH.

b. Next, estimate the network's hourly energy consumption assuming all mining is done on an Antminer Hydra that has a hash rate of 18 terra-hash/sec and consumes 1.7 kW of power (running the device for an hour consumes 1.7 kWH of energy). Assume the current difficulty of generating a bitcoin block is $D = 2^{75}$.

c. Explain why there is such a large gap between the two estimates.

Problem 5. Two business partners devise the following cold storage scheme for Bitcoin such that both partners must consent to withdrawing any funds: They generate an ordinary P2PKH address for the funds. Then, they print the address's private key as a QR code on a piece of paper, slice the QR code in half with a paper cutter, and give each partner one half of the paper to store. They test this scheme extensively and establish that they will always be able to reconstruct the QR code from the two halves.

a. Explain how one business partner, if malicious, can unilaterally withdraw Bitcoin from cold storage without consent of the other partner. Recall that Bitcoin uses the ECDSA signature scheme where a private key is a 256-bit integer. Use the fact that QR codes contain enough redundancy that one can recover 3/4 of the bits from a half of the image.

b. How should the business partners have implemented their cold storage to achieve their goals?

Problem 6. In lecture 5, we saw that Casper rewards miners who stake a deposit and vote for links $s \to t$ by signing messages of the form $\langle v, s, t, h(s), h(t)\rangle$. Here v is the miner's identity, s (source) and t (target) are hashes of checkpoint blocks, $h(s)$ and $h(t)$ are the heights of the checkpoints, and s is an ancestor of t in the blockchain. A *supermajority link* $s \to t$ is one that receives votes from more than 2/3 of miners (by stake). We say a block t is *justified* if t is the genesis block or there is a justified s such that $s \to t$ is a supermajority link. A block s is *finalized* if s is justified and there is a t such that $h(t) = h(s) + 1$ and $s \to t$ is a supermajority link.

A miner v who signs both $\langle v, s_1, t_1, h(s_1), h(t_1)\rangle$ and $\langle v, s_2, t_2, h(s_2), h(t_2)\rangle$ gets *slashed* (loses its deposit) if either of two conditions holds:

- $h(t_1) = h(t_2)$ but $t_1 \neq t_2$ (voted for two target blocks at the same height), or
- $h(s_1) < h(s_2) < h(t_2) < h(t_1)$ (voted for one link nested within another)

Assume that more than 2/3 of miners (by stake) are honest and never get slashed, and suppose miners finalize blocks a_m and b_n, where $h(a_m) < h(b_n)$. Let $r \to a_1 \to a_2 \to \cdots \to a_m \to a_{m+1}$ and $r \to b_1 \to b_2 \cdots \to b_n \to b_{n+1}$ be supermajority links that caused a_m and b_n to be finalized, where r is the genesis block. Prove that a_m is an ancestor of b_n.