ECE 598PV Principles of Blockchains Assignment 3

Date Assigned: April 9, 2020
Date Due: April 16, 2020

Abstract. In her/his seminal paper, Nakamoto considered a specific type of attacker behavior where the attacker starts at a specific block (kept to be Genesis in this homework) and mines a chain in private and releases/broadcasts the chain when its length overtakes the (public) longest chain and the length of the public chain is greater than a parameter k. This behavior can encode a double-spend transaction and is thus a fatal attack on the protocol; we henceforth denote this as the *Nakamoto attack*. Nakamoto used the Poisson model of mining and calculated the probability of success of this attack as a function of the depth of the private chain (also the depth of the fork) when released; he noted that the probability decreases exponentially as a function of the depth. In this homework we explore these attacks in detail via simulations of the type Nakamoto initiated.

Model. In all the experiments below we consider only two parties: one adversarial (with hash power fraction β) and honest (with hash power $1-\beta$). By allowing the distributed honest parties to "congregate", we have essentially assumed infinitesimal network delay. Time is modeled as a continuous variable. At any time, the adversary selects any block to mine and succeeds at a random time exponentially distributed with mean $\frac{1}{\beta}$. If the adversary selects a different block to mine on before this time, then the previous mining effort is discarded and the mining operation refreshes: success of mining on this new block occurs at a random time exponentially distributed with mean $\frac{1}{\beta}$. When an adversary succeeds in mining, it can either make the block *public* or hold it in *private*. The selection of which block to mine at any time, as a function of the current blocktree, constitutes the space of adversarial strategies.

The honest party has access to the public blocktree (composed of the blocks released by the honest party together with those publicly released by the adversary) and at any time, mines on the tip (leaf) of the longest chain in the public blocktree. If there is more than one longest chain, then the adversary controls how the honest party's mining power is split across the multiple longest chains.

Questions.

1. Suppose the adversary always holds the mined blocks in private and selects to mine only on its' private chain. Thus there are two chains, forked at the genesis: the public one (mined on by the honest party) and the private one (mined on by the adversary). The adversary is successful if **it's privately held chain of blocks is longer than the honest chain and the honest chain is longer than a parameter** k. This strategy of the adversary is the Nakamoto private attack: it is successful in encoding a double-spend if k is larger than the depth of the confirmation rule followed by the honest party. Recreate this attack via a simulation and plot the probability of success (in log scale) as a function of k. Conduct this plot for different values of adversarial hash power $\beta = 0.1, 0.2, 0.3, 0.4$. Also conduct this plot for $\beta = 0.6$; discuss the differences in your plots for $\beta < 0.5$ and $\beta > 0.5$. *Note*: This question can be answered via mathematical calculations (as Nakamoto did) or via an event driven simulation testbed (the probability of success of the attack is empirically estimated by conducting many i.i.d. mining experiments, each restarting from the Genesis). We recommend answering this question using an event driven simulation testbed that can be reused in the later questions. For the simulation, use a stopping time (eg: when the public chain has length $\max(k + 100, 2k)$) such that the standard deviation associated with the empirical success probability estimate is sufficiently small.

2. An alternative type of adversarial behavior is the following, that we call a *balance attack*: the adversary mines in such a way as to maintain two forks of as equal length as possible. The adversary behavior is the following, where there will be just two chains in the blocktree, forked from Genesis:

   - Adversary always publicly releases any successfully mined block.
   - If the two chains are of unequal length, then the adversary always works on the shorter of the two chains.
   - If both the chains are of equal length, the adversary does not mine. Further, the adversary forces the honest party to split its mining equally among the two chains.

   Some observations:

   - At the beginning, the only block is Genesis and we consider this situation analogous to two equally long chains and the adversary does not mine, waiting until the honest party successfully mines a block over the Genesis.
   - When the two chains are of equal length, only the honest party is mining (on both the chains) and as soon as one of the two chains grows in length, then the symmetry is broken. At that point in time, both the adversary and honest party reset the blocks they are mining on (the honest party mines on the longer of two chains and the adversary on the shorter one).

   We say this attack is successful if **there exists a point of time where both chains are of equal length greater than** k. Conduct a simulation of the balance attack and plot the probability of success (in log scale) as a function of k. Conduct this plot for different values of adversarial hash power $\beta = 0.1, 0.2, 0.3, 0.4$. Also conduct this plot for $\beta = 0.6$; discuss the differences in your plots for $\beta < 0.5$ and $\beta > 0.5$. How does the balance attack compare to the private attack?

3. The adversary strategy space has two different dimensions:

   - where to mine a block;
   - when to publicly release a successfully mined block.

   In the private attack, both dimensions were utilized: the adversary mines on its private chain and releases the full private chain only when the honest chain has grown to length k. However, in the balance attack above the second dimension was not fully explored: the adversary publicly released its block as soon it successfully mined it. In this question, we explore a more nuanced version of the balance attack, where again there are only two chains in the blocktree (forked from Genesis):

   - If the two chains are of unequal length, then the adversary always mines on the shorter of the two chains; the honest party mines on the longer of the two chains (following the longest chain protocol).
   - If both the chains are of equal length, then the adversary picks one chain to mine on, and forces the honest party to mine on the other chain. If the honest party succeeds in mining first, then the chains are of unequal length and we return to the previous step. If the adversary succeeds in mining first, then it holds the block in private and stops mining until the honest party successfully mines a block. At that point, the adversary publicly releases its block and the two chains are again of equal length.

We say this attack is successful if **there exists a point of time where both chains are of equal length greater than** k. Conduct a simulation of the balance attack and plot the probability of success (in log scale) as a function of k. Conduct this plot for different values of adversarial hash power $\beta = 0.1, 0.2, 0.3, 0.4$. Also conduct this plot for $\beta = 0.6$; discuss the differences in your plots for $\beta < 0.5$ and $\beta > 0.5$. How does this nuanced balance attack compare to the earlier version?

4. **Bonus**. Can you further enhance the balance attack specification? Experimentally evaluate the performance of your enhancement. *Hint*: Instead of stopping mining (when it had a one-block private lead over the honest party's efforts), the adversary could continue to mine in private, potentially building an even longer lead.

5. **Bonus++: for the theoretically inclined student**. What is the optimal adversary strategy in terms of probability of success, for any fixed k?