Department of Electrical Engineering
Sharif University of Technology

Foundations of Blockchain
by: Dr. Mohammad A. Maddah-Ali
Fall 1399(2020)

Problem Set 4

If you have any questions about the problems please contact at this email address : kasraabbaszadeh@gmail.com

Question 1: In Bitcoin paper, security is analyzed under a discrete model based on gambler's ruin problem.

a) Explain the problem, it's solution and relation to bitcoin.

b) Consider Nakamoto's private attack, calculate Error probability of k-deep confirmation rule under this attack using the results of part (a).

c) Argue whether this model is a complete or not.

Question 2: Consider another attack which is Nakamoto's private attack combined with a pre-mining phase. The attack is focused on reverting a transaction TX included in the i-th block of the public chain.

Pre-mining phase: Starting from the genesis block, the attacker starts mining blocks in private to build a private chain. When the first honest block h_1 is mined on the genesis block, the attacker does one of two things: i) If the private chain is longer than the public chain at that moment, then the adversary continues mining on the private chain; ii) if the private chain is equal or shorter then the public chain, the attacker abandons the private chain it has been mining on and starts a new private chain on h_1 instead. The attacker repeats this process with all honest blocks h_2 ,h_3 , . . . h_{i-1}.

Private attack phase: After block h_{i-1} is mined, the attacker will start Nakamoto's private attack from the current private chain it is working on, whether it is off h_{i-1} or the one it has been working on before h_{i-1} depending on which is longer.

a) Suppose fraction of adversary mining power as $\beta < 0.5$. What is the probability that the attacker will switch to h_1 when it is mined? What is the expected depth at which the attacker is mining when h1 arrives?

b) Let N^a_{i-1} be the depth at which the adversary is mining just before the $(i-1)$th honest block arrives. Let $G_{i-1} = N^a_{i-1} - i + 1$ the advantage the adversary has over the public chain. The distribution of G_{i-1} depends on

i. Explain what happens when i is too large? (no need for mathematical proof)

c) Argue that this attack is strictly stronger than the pure Nakamoto's private attack.

bonus) Use Monte Carlo simulation and simulate this attack for large i and estimate the confirmation error probability for k = 5, 10, 15, 20 and adversarial hash power fraction $\beta = 0.3$. (provide your code and results in the solution)

Question 3: Now, lets try another continuous model for analyzing Bitcoin. As you know mining blocks is Poisson process with λ rate.

a) What is a reasonable model for the distribution of blocks inter-arrival time ? Explain. What is the variance of this time under your model?

b) Consider Nakamoto's private attack and let E_k be the event that the adversary mines k blocks before the honest miners mine k blocks. Based on part (a) what is the probability of E_k when k is large enough?

c) Using Chernoff bound or otherwise, give an upper bound to E_k . Explicitly give the exponent in your bound.

d) Now give an upper bound for Error probability of k-deep confirmation rule and show it exponentially decreases with k.

Question 4: Here we study a different confirmation rule and compare its performance with the k-deep rule under the private attack. In this confirmation rule, which we will call a t-wait rule, we confirm a block b, t seconds after the block has been mined.The adversary starts mining a private chain from the parent of b immediately after b is mined. Let λ be the total mining rate, of which β fraction belongs to the adversary

a) Define P_t the event that the adversary mines more blocks than honest nodes in time t after starting attack. Give an exact expression for the probability P_t that the adversary has an equal or longer chain than the honest chain at confirmation. Your expression can involve an infinite summation.

Hint: the moment-generating function of a Poisson random variable
$M_{(\lambda)}(\gamma) = exp(\lambda(exp(\gamma) - 1))$

b) Using Chernoff bound or otherwise, give an upper bound to P_t to show that it decreases exponentially with t. Explicitly give the exponent in your bound.

c) The confirmation latency of this rule is obviously t seconds, a deterministic quantity. The latency of the k-deep confirmation rule is however random. What is the expected value of the latency? By matching this expected value to t, compare the performance of the two confirmation rules, in terms of the rate of exponential decrease in confirmation error probability.

Question 5: Consider Bitcoin-NG protocol and suppose there exists a miner whose mining power ratio out of all mining power in the system is β. Denote by r_{leader} the revenue of the leader from a transaction, leaving $1 - r_{leader}$ for the next miner. assume $r_{leader} = 40\%$.

a) The adversary can potentially improve his revenue to earn 100% of the fee by withholding his microblocks. Explain the scenario and achieve β^* under this attack and compare it with β^* in nakamoto's consensus.

b) Also there is another way to increase revenue. a miner could avoid the transaction's microblock and mine on a previous block to include transactions in his own blocks and earn 100% of the fee. Again achieve the β^* and compare it with the last attack.

Question 6: Consider GHOST protocol under the balance attack. adversary is trying to divide the chain into k sub-trees. Let λ_c the rate of mining blocks in each sub-tree and λ_a the rate of mining adversary blocks.

a) Define X_i as length of sub-tree i and $D := Max|X_i - X_j|\ \forall i, j = 1, ..., k$. Using Chernoff bound or otherwise, give an lower bound for $Pr(D < \delta\lambda_c)$ in terms of δ.

(Hint :$Pr(X > (1+\delta)\mu) < exp(-(\delta^2/3)\mu)$, $Pr(X < (1-\delta)\mu) < exp(-(\delta^2/2)\mu))$

b) Let $\delta = (\lambda_a - 1)/(2\lambda_c)$ and show that the expected number of adversary blocks attacker can mine is strictly greater than what he needs to keep chains balance, with high probability.

Question 7: In Prism protocol we have 3 types of blocks : transaction block, proposer block, voter block. let q_k be the probability that there is a "reversal error" with Voter Block at level k. Reversal error is the exact same as a k-deep confirmation error in the longest chain protocol. We define effective vote for a Proposer Block from Voter chain i at time t as $v_i(t) = 1 - q_{ki}(t)$ and the number of votes a proposer block has at time t as $H(t) = \Sigma v_i(t)$.

a) Let m be the number of voter chains, and λ_h be the rate at which honest nodes mine blocks on each voter chain. Suppose the public proposer block arrives at time 0. At time $t > 0$, compute the expected fraction of voter chains that have voted on this block when m is large enough.

b) Compute the expected number of voter chains for which the vote is k-deep at time $t > 0$, in terms of k.

c) Using the earlier parts or otherwise, give an expression for H(t), valid asymptotically for large m, in terms of the reversal probabilities q_k.

References

[1] S. Nakamoto. *A Peer-to-Peer Electronic Cash System* , 2008.

[2] I. Eyal, A. Efe Gencer, E. Gun Sirer, R. van Renesse. *Bitcoin-NG: A Scalable Blockchain Protocol* , 2015.

[3] Y. Sompolinsky and A. Zohar. *Secure High-Rate Transaction Processing in Bitcoin* , 2015.

[4] V. Bagaria, S. Kannan, D. Tse, G. Fanti, P. Viswanath. *Deconstructing the Blockchain to Approach Physical Limits* , 2015.