ECE 595: Foundations of Blockchain Systems **October 26, 2020**

Lecture 8

Lecturer: Sreeram Kannan *Scribe: Hao Yin*

Outline: This lecture mainly focus on the full security proof. First, the general pre-mining attack is introduced. The general pre-mining attack includes two phases: Pre-mining phase and private attack phase. Then, A full security proof of longest chain given $\Delta = 0$ is showed. The safety violation implies the contradiction based on the statistical claim, which proves the confirmation policy (k-Deep Policy).

8.1 Beyond the Private Attack

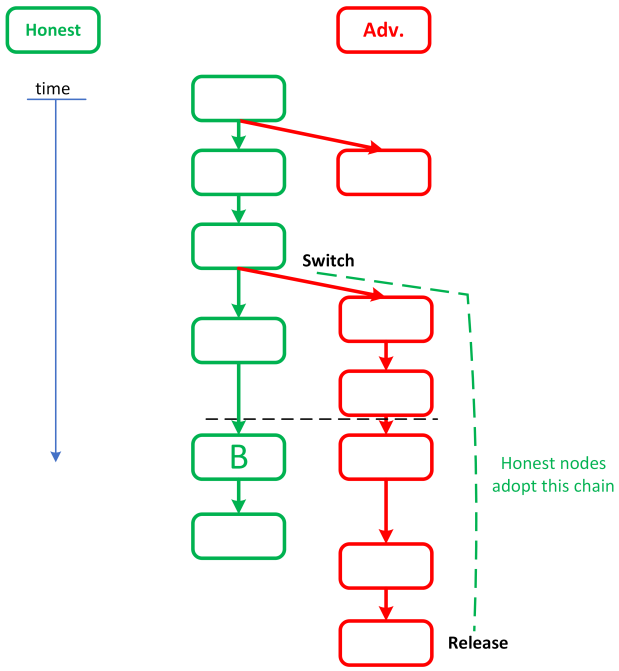

Figure 8.1: Illustration of the pre-mining attack.

In reality, we have the following scenario shown in Fig. 8.1. We have a bunch of blocks and the goal is to confirm a certain block B. It's not only the case that the adversity can build the chain starting at the red chain, but the adversity could have also built a chain starting at a different position (red chain). If you had enough blocks, it could still outdraw B.

8.1.1 General pre-mining attack

Pre-mining phase: Pre-mining phase starts from genesis of a private chain. This phase starts before B is mined. The adversary tried to maintain a lead over the public chain, if the adversary is no longer in leading position, i.e., the private chain is shorter than the public chain, it will switch to start a new private chain on the top of public chain. Hence, the adversary could come back to a leading position potentially. This implies that the adversary is always trying to maximize its current lead over the public chain, so when B is mined, it just focuses on trying to revert that block. How much the adversary can have a lead at a given time is just like the process of random walks. Those random walks generally have a nontrivial distribution.
Private attack phase: This phase starts after block B is mined in public. At this point that B was mined, the adversary does not switch anymore and continues on the same chain. At some point the adversity has a chain k longer than the honest chain and then it will release this one. So then what will happen is that all the honest nodes will adopt this chain.

8.1.2 Balance attack

Balance attack is also possible, the adversary keeps trying to balance the two chains. Different nodes will have different longest chain. The adversary keeps making sure that there are chains with the same length, so the honest nodes are confused about which is the longest chain as there is no unique longest one. An illustration is shown in Fig. 8.2. The Balance attack: an attacker transiently disrupts communications between subgroups of similar mining power. During this time, the attacker issues transactions in one subgroup, say the transaction subgroup, and mines blocks in another subgroup, say the block subgroup, up to the point where the tree of the block subgroup outweighs, with high probability, the tree of the transaction subgroup. The novelty of the Balance attack is to leverage the GHOST protocol that accounts for sibling or uncle blocks to select a chain of blocks. This strategy allows the attacker to mine a branch possibly in isolation of the rest of the network before merging its branch to one of the competing blockchain to influence the branch selection process [2].

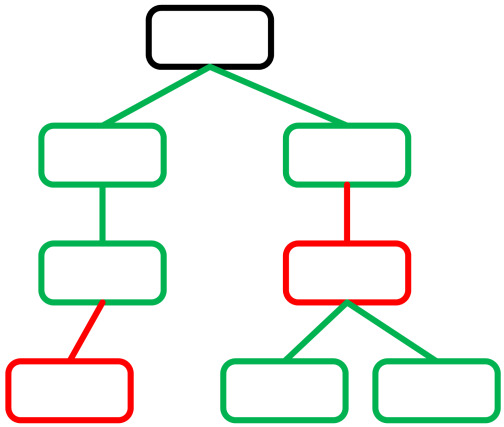

Figure 8.2: Illustration of the balance attack

8.2 Full security proof of longest chain

Let us first denote λ_h is the honest mining rate, λ_a is the adversary mining rate, and Δ is the network latency. The are two things for security: One is called safety, another is called liveness. Safety means the confirmed transactions remains confirmed while liveness means new honest transactions will be eventually confirmed.

8.2.1 Safety violation

Let us first start with $\Delta = 0$, with an example illustrated in Fig. 8.3. Assume safety is violated:

1. Block B is k-deep inside the longest chain of a honest node.
2. The competing chain (excluding B) becomes longer.

The safety violation implies that $\lambda_a > \lambda_h$ with high probability. Here is an important fact when $\Delta = 0$: If a block is born at level l, there is No other honest block at level l. In Fig. 8.3, if we examine two chains after B_0, each level after B_0 can be categorized into two scenarios:

1. Both blocks are adversaries.
2. One block is adversary, and the other is honest block.

The impossible scenario: Both are honest blocks. These two scenarios imply:

1. l_0 blocks between B_h and B_0 are adversaries (because B_h is the latest honest block before B_0).

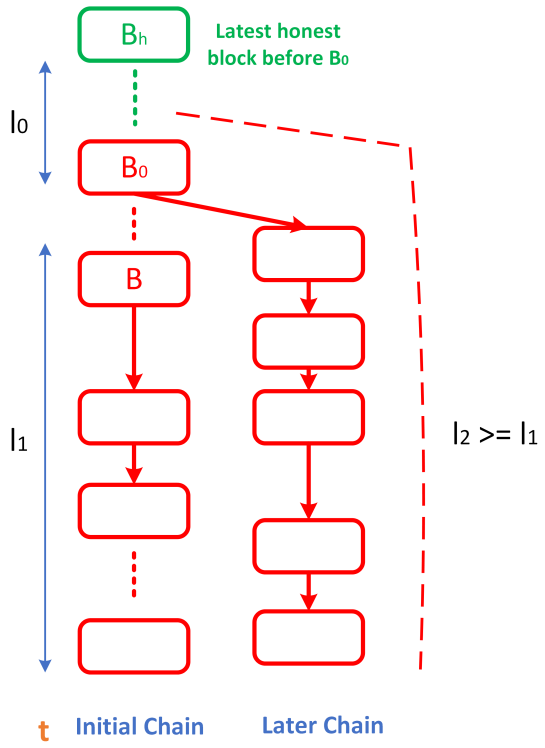

Figure 8.3: Illustration of the safety violation.

2. In each of the later levels, at least one block is adversary.

Therefore, $l_0 + l_1$ adversary blocks are created between the instant when B_h was mined and now. Note that the adversary blocks could not have born before τ_h, where τ_h is the time when B_n was born. Assume the current time is t, there are at least $l_0 + l_1$ adversary blocks between τ_h and t while there are at most l_1 honest blocks. Therefore, safety violation implies that the number of adversary blocks is greater or equal to the number of honest blocks between τ_h and t.

Statistical claim 1: If $\lambda_h > \lambda_a$ in any sufficient long duration η, for any $(t, t+\eta)$, the number of mined adversary blocks is less than the number of honest blocks except with small probability. Thus, if $t - \tau_h > \eta$, we can use the statistical claim to get contradiction. In other words, safety violation implies the contradiction, which means there is no safety violation.

Statistical claim 2: If k (blocks) is chosen correctly (large enough), $t - \tau_h > \eta$ with high probability. (idea: $t - \tau_h >$ time for $k-$blocks to be bound $> \eta$ with high probability)

Here, what we are analyzing is to prove that there exists an appropriate parameter k under which the safety violation will not occur unless $\lambda_a > \lambda_h$.

Confirmation Policy (k-Deep Policy): If B is in my longest chain, and k blocks are below B in the

longest chain, then B is confirmed [1].

References

[1] Juan Garay, Aggelos Kiayias, and Nikos Leonardos. The bitcoin backbone protocol: Analysis and applications. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 281–310. Springer, 2015.

[2] C. Natoli and V. Gramoli. The balance attack or why forkable blockchains are ill-suited for consortium. In *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pages 579–590, 2017.