Probability in Bitcoin's Blocks Chasing

Ze Sen Tang
Southern Arkansas University
Magnolia, AR. USA

Elgaddafi Elamami
Southern Arkansas University
Magnolia, AR. USA

Abstract

To prove bitcoin's security system works, we have to make sure that the honest chain will never lose in the blocks chasing with the attacker chain. To solve this problem, we propose the Binomial Distribution as a solution that show the probability of the attacker chain catch up the honest chain.

Keywords: Bitcoin, Binomial distribution, Block chasing.

1. Introduction

Bitcoin's security system is a partly based on the assumption of the blocks chasing problem. Satoshi stated that "the system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.(1)" In the calculation, we have to prove the probability of the attacker chain will catch up the honest chain is infinitively near to zero.

2. Probability for Next Block

In the chasing of both sides, there is a probability for both sides to find the next block, giving (6):

$$p = theprobabilityofanhonestnodetofindthenextblock$$

Since the attacker will not find the block when the honest node found it, then:

$$q = theprobabilityofanattackertofindthenextblock$$

Thus, when p is greater than q, it means the honest nodes occupied more CPU power than attacker nodes; when q is greater than or equal to p, it means the attacker nodes occupied more CPU power than the honest nodes.

The race between the honest chain and an attacker chain can be characterized as a Binomial Random Walk. The success event is the honest chain being extended by one block, increasing its lead by +1, and the failure event is the attacker's chain being extended by one block, reducing the gap by -1 (Satoshi 6).

In this article, we can assume

$$z = thenumbersofblockthattheattackerlagbehindthehonestnodes$$

Since the probability of an honest node to find the next block is p and the probability of an attacker to find the next block is q, the probability of the attacker will catch up the honest chain when the attacker is z blocks behind is presented as q_z:

$$q_z = \left(\frac{q}{p}\right)^z, if q < p$$

$$q_z = 1, if q \geq p$$

Since we are given that the honest nodes occupied more CPU power than the attacker nodes, q must be smaller than p and, thus, when time goes on, the probability of the attacker will catch up will come infinitively near to zero

$$\lim_{z\to\infty}(\frac{q}{p})^z = 0, if q < p$$

We have shown that the probability of the attacker chain will catch up the honest chain is infinitively near to zero when z is infinitively closed to infinity. So, to make this situation possible, we have to make $z \to \infty$ and $q < p$. The situation $q < p$ is given; however, $z \to \infty$ is impossible to accomplish since the user cannot wait for infinite time in the process. Then, to prove this system works, we have to show how long the user should wait until the probability of the attacker chain will catch up the honest chain is a pretty closed to zero.

Therefore, to show the probability of the attacker chain will catch up the honest chain at a certain time period, we have to know how far the attacker chain will go in that time. Then, we use Poisson distribution to find it. First, we find the expected number of the attacker blocks, which equalsto:

$$\lambda = z\frac{q}{p}$$

Then, we can find the probability of the progress of attacker has made by using Poisson distribution.

$$let k = the number of blocks the attacker has made$$
$$and P(B_k) = the probability that the attacker has made k blocks$$
$$P(B_k) = \frac{\lambda^k \cdot e^{-\lambda}}{k!}$$

Finally, we can calculate the probability of the attacker will ever catch up at certaintime period.$let A = the event that the attacker will ever catch up$
Then, we just use the law of total probability:

$$P(A) = \sum_k P(A|B_K)P(B_k)$$
$$P(A) = \sum_{k=0}^{\infty} \frac{\lambda^k \cdot e^{-\lambda}}{k!} \cdot \begin{cases} (\frac{q}{p})^{(z-k)}, if z \geq k \\ 1, if z < k \end{cases}$$

To avoid infinity, we rearrange the equation:

$$P(A) = 1 - \sum_{k=0}^{z} \frac{\lambda^k \cdot e^{-\lambda}}{k!} \cdot (1 - \left(\frac{q}{p}\right)^{z-k})$$

In this equation, we can see the relation between p and q has a great influence to the result. The closer the value of q to p, the longer the time needs to be wait by the user.

4.Conclusion

Bitcoin's blocks chasing security system is greatly dependent to the relation of time and CPU power. The equation shows that a short-term operation needs a significant small value of q; however, since the value of q is uncertain, the time needs to be wait by users is always unclear too. Thus, with a higher probability of getting into the trap of attacker with wrong time prediction, Satoshi's statement of "the system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes (1)" is not enough with an unclear value of q.

5. References

[1] Feller W. ," An introduction on probability theory and its applications,"1957.
[2] Nakamoto S., Bitcoin: A peer to Peer Electronic Cash System, www.bitcoin.org, 2008
[3] The probability behind Bitcoin, https://math.stackexchange.com/questions/2356763/the-probability-behind-bitcoin
[4] Triola M., Elementary Statistics, 13th edition, 2014