Advances in Intelligent Systems Research, volume 147

International Conference on Network, Communication, Computer Engineering (NCCE 2018)

Mathematical Derivation and Analysis of Success Probability of Bitcoin Attack

Yingyu Pan

School of Beijing University of Posts and Telecommunications, Beijing 100876, China.

qearlyy@sina.com

Abstract. By using block chain technology, bitcoin has realized a real de centralization and point to point digital currency system, which effectively solved the problems of "double payment" and "curbing inflation". Bitcoin has the value and function of money, therefore, in practical application, we need to consider one problem -- "malicious attack", whose success probability affects the basic security performance of the system. This paper is based on the mathematical derivation and analysis of the model and formula given by the "Bitcoin: A peer-to-peer electronic cash system" in the original paper of Satoshi Takemoto's paper. And verify the theoretical guarantee that the success of attack needs the following conditions: Mastering the calculation power of "50%".

Key words: Bitcoin; Block Chain; The Success Probability of Attack; Mathematical; 50% Computational Force.

PREFACE

In order to solve many problems in the "centralization" management needed for the basis of trust in the transaction, Santosh Takemoto proposed a digital currency, "bitcoin" in 2008. With the continuous development of this "de centralization" concept and the promotion of the value of "bitcoin" digital money, more and more people begin to pay attention to "bitcoin" and block chain technology, making it a hot spot of current research. In such a pure digital currency system, security is particularly important, and the probability of a "malicious attack" and the conditions it needs also play a decisive role. At present, there are many research results on the security of bitcoin system under this topic. This paper mainly studies the probability of successful attack on the system. Through the corresponding mathematical model, the probability formula is derived from the basic principle, and the probability changes are simulated and the results are analyzed.

BITCOIN TRADING

Bitcoin transactions are similar to traditional cash transactions, that is, the transaction itself is P2P. But the difference is that the bitcoin transaction is not a real time confirmation transaction. It needs to be confirmed after the transaction is written to the block by "miners" through the broadcast of the information to the whole bitcoin network. After the block is generated, the block chain is added. After each block is added, the transaction of the block is verified, so as to ensure the authenticity of the transaction.

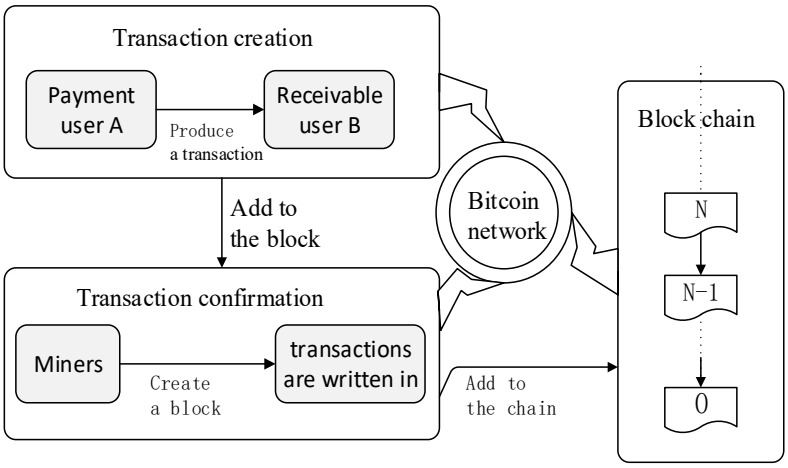

FIGURE 1. Bitcoin Trading Model.

ATTACK AND THE PROBABILITY OF SUCCESS

In the course of the transaction, if an attacker launched an attack (it is assumed that the payment user A is a malicious attacker), it is impossible for him to create a new bitcoin in the bitcoin system, or to obtain a bit of bitcoins from other users. What he can do is to achieve the purpose of "double payment", that is, after paying the B users, he will get the bitcoin for his own use again. To do this, the attacker needs to create a chain faster to replace the current honest chain starting with the transaction information. At this point, the problem is transformed into a "race" between the attack chain and the honest chain.

To achieve "double payment", the payment user A (attacker) first makes the receiver B believe that he has paid the money, then he will get the money back after a while. In order to calculate the probability of attack success probability P, we first need to calculate the probability of the K long attack chain generated at this time point, and then the probability of "catching up" in the attack chain is calculated in the case of the gap between the honest chain and the N data block, and the multiplication is the probability of attack success:

$$P = p_k * q_n$$

The Probability of Producing K Long Attack Chain

In bitcoin transactions, the receiver generates a pair of new keys before signing, and then sends the public key to the sender quickly. This avoids the sender's attempt to prepare a block of data blocks in advance and work continuously to exceed the integrity chain. At this point, the attack chain can only start after the transaction is created. The occurrence of attack chain is similar to Poisson process: the number of events occurring in two non-overlapping time intervals is independent random variables.

$$p_k(t) = \frac{(\lambda t)^k}{k!} e^{-\lambda t}$$

If time t is a definite value, the formula can be written as:

$$p_k = \frac{(\lambda)^k}{k!} e^{-\lambda}$$

Hypothesis: p is the possibility of finding the next block of data for honest nodes.

Q is the possibility of finding the next block of data for attackers and has iPAQ=1.

At the time point of determination, the mathematical expectation of honest chain length is Zandt then the mathematical expectation of attack chain length k is:

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

The probability that the length of the attack chain is k is:

$$p_k = \frac{(\lambda)^k}{k!}e^{-\lambda}$$

In that case, the difference between the honest chain (Z length) and the attack chain (k length) is z-k data blocks.

The Probability of the Attack Chain Catch Up the Honest

Based on the above assumptions and calculations, we consider the probability of catch up gap n. The problem is similar to "drunkard hovering":

FIGURE 2. Model of hovering problem of drunkard.

When p is less than q, q_n =1; consider p>q:

In this model, if the drinker is at a certain is, when the time scale is small enough, the next position may be only i-1 or i+1, and there is no jump at a position greater than 1. The probability of one step to i-1 (decreasing to the left shift) is p to is (to the right shift gap) q. The moving process can be translated into three position changes:

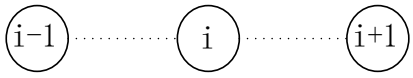

FIGURE 3. Equivalent position diagram.

At this point, the probability P (is) is shifted from is to i-1 that the probability of q moving to the left plus the probability of moving one step to the right is multiplied by the probability from i+1 to i-1:

$$P(is) = q + p * P(i+1) \quad (1)$$

The probability P (i+1) at i+1 to i-1 can be viewed as Figure 3, and the state translates to is---i+1---i+2, which is equivalent to two (1) multiplication:

$$P(i+1) = Phi) * Phi) \quad (2)$$

And (2) together, and iPAQ=1; can be solved:

$$P(i+1) = \frac{q}{p}P(is)$$

It is delivered by this type and has P (0) =1; the general solution can be obtained:

$$q_n = \begin{cases} 1 & p \leqq q \\ \left(\frac{q}{p}\right)^n & p > q \end{cases}$$

The gap n should be minus the attack chain length for the honest chain length, that is, n=z-k.

The Probability of a Successful Attack P

From the above two parts, we can deduce the probability of successful attack in each case of k:

$$P = \sum_{k=0}^{\infty} \frac{(\lambda)^k}{k!} e^{-\lambda} \bullet \begin{cases} 1 & k>z \\ \left(\frac{q}{p}\right)^{z-k} & k \leqq z \end{cases}$$

Avoid infinite sum and variable limit operation in simulation:

$$P = 1 - \sum_{k=0}^{z} \frac{(\lambda)^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right) \tag{3}$$

MATLAB Simulating

MATLAB is used to solve the success probability of attack on the z gap corresponding to different q values:

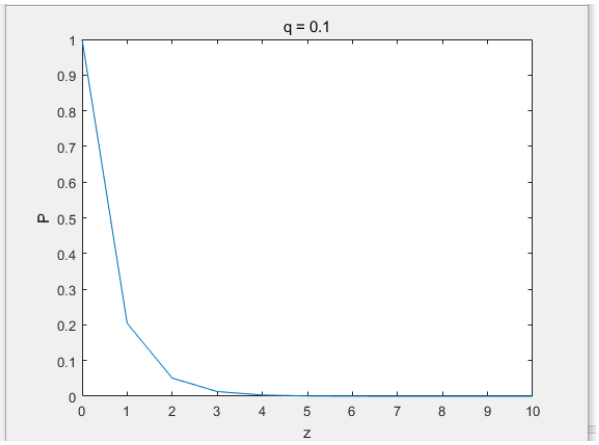

FIGURE 4. Z-P images in the case of q=0.1.

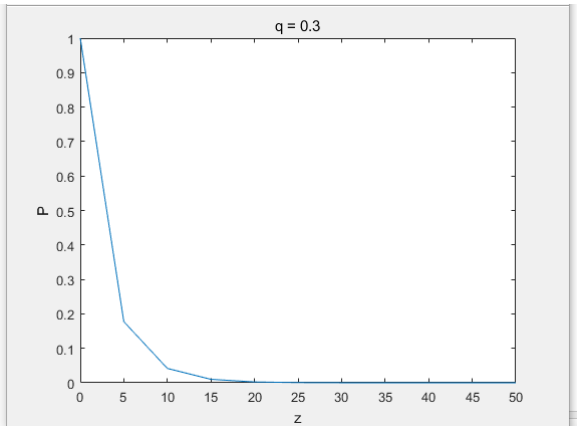

FIGURE 5. Z-P images in the case of q=0.3.

PROBABILITY ANALYSIS OF ATTACK SUCCESS

From the above deduction, it can be concluded that under the condition of $q<p$, the probability of successful attack will decrease sharply with the increase of z. And when the z value is not large, the probability of successful attack is basically zero.

According to probability expression (3), it is possible to ensure that the condition of attack success theoretically reaches 50% for the attacker. Considering the broadcast time in practical practice, the actual attacker's calculation power will be slightly biased. To meet this computing power demand, the attacker's funds are very uneconomical compared with the miner's work on the "incentive" mechanism in the bitcoin.

CONCLUSION

The technology of block chain, which is derived from bitcoin, is getting more and more attention, and the security of digital money economy under this technology is becoming more and more important. The calculation process of attack success probability involves Poisson process and other mathematical models, and some of them are difficult to understand. Based on the basic mathematical principle, this paper uses the model relation graphics to deduce the probability of success in the attack and uses software simulation to analyze and draw the conclusion directly. The security of bitcoin system also involves encryption algorithm, transaction verification, and software security and so on.

REFERENCES

1. Takemoto Bitcoin: A peer-to-peer electronic cash system[R].2008, p.6-8.
2. Yahoo Chen, ChunYan Sun. The probability of a gambler's bankruptcy [J].1992(02):36-39.
3. Ping Wang. On Poisson process [J].CD-ROM technology, 2008(04):17-19.