Association for Information Systems

AIS Electronic Library (AISeL)

ICEB 2016 Proceedings

International Conference on Electronic Business (ICEB)

Winter 12-4-2016

A Probability Model for Analysis of Attacks on Blockchain

Ming-hua Hsieh
National Chengchi University, mhsieh@nccu.edu.tw

Ming-Tao Chung
National Chengchi University, 102356509@nccu.edu.tw

Yan-Ping Chi
National Chengchi University, ypchi@mis.nccu.edu.tw

Recommended Citation

Hsieh, Ming-hua; Chung, Ming-Tao; and Chi, Yan-Ping, "A Probability Model for Analysis of Attacks on Blockchain" (2016). *ICEB 2016 Proceedings*. 41.
https://aisel.aisnet.org/iceb2016/41

A PROBABILITY MODEL FOR ANALYSIS OF ATTACKS ON BLOCKCHAIN

Ming-hua Hsieh, National Chengchi University, mhsieh@nccu.edu.tw
Ming-Tao Chung, National Chengchi University, 102356509@nccu.edu.tw
Yan-Ping Chi, National Chengchi University, ypchi@mis.nccu.edu.tw

ABSTRACT

In a blockchain, the longest chain, which has the greatest proof-of-work effort spent in it, represents the majority decision. To change the transaction data of a block, an attacker has to control more computing power than other honest nodes. This situation can happen if the attacker can hack into the systems of honest nodes. To analyze the probability of such event, we propose a probability model for analysis of attacks on blockchain. The model is based on the structure of a peer-to-peer network. We assume the state of each honest node follows a two-state (hacked or normal) Markov chains. A hacked node is assumed to be controlled by the attacker and its computing power belongs to the attacker. On the other hand, the computing power of a normal node belongs to the honest longest chain. We apply the model to study the probability of the majority decision is controlled by the attacker and the duration of such event. In addition, we analyze the magnitude of the loss for such event.

Keywords: Blockchain, the longest chain, blockchain attack, Markov chain, stochastic process

INTRODUCTION

Bitcoin has emerged as the most successful cryptocurrency. According to http://blockchain.info/charts/market-cap, the Bitcoin market capitalization is over 100 billion US Dollars as of October 2016. The coins of bitcoin network are created from the network protocol directly, without any central authority involved. Most of these economic value is generated from this innovation. As of October 24, 2016, the bitcoin blockchain wallet user is near 10 millions and daily USD transaction value is more than 120 millions on average (see Fig. 1). The computing power of the bitcoin network is greater than any supercomputer on earth. The current computing power is more than 2000 peta-hash per second (see Fig. 2). Bitcoin is not just a virtual currency, it is a collection of concepts and technologies. Bitcoin was designed by software developers without apparent influence from financial industry or regulators. A key idea in bitcoin network is Proof-of-Work. A mining node shows its Proof-of-Work by solving a difficult cryptography puzzle and get rewarded. Therefore, the probability of receiving reward of each mining node is proportional to its computing power/hash rates.

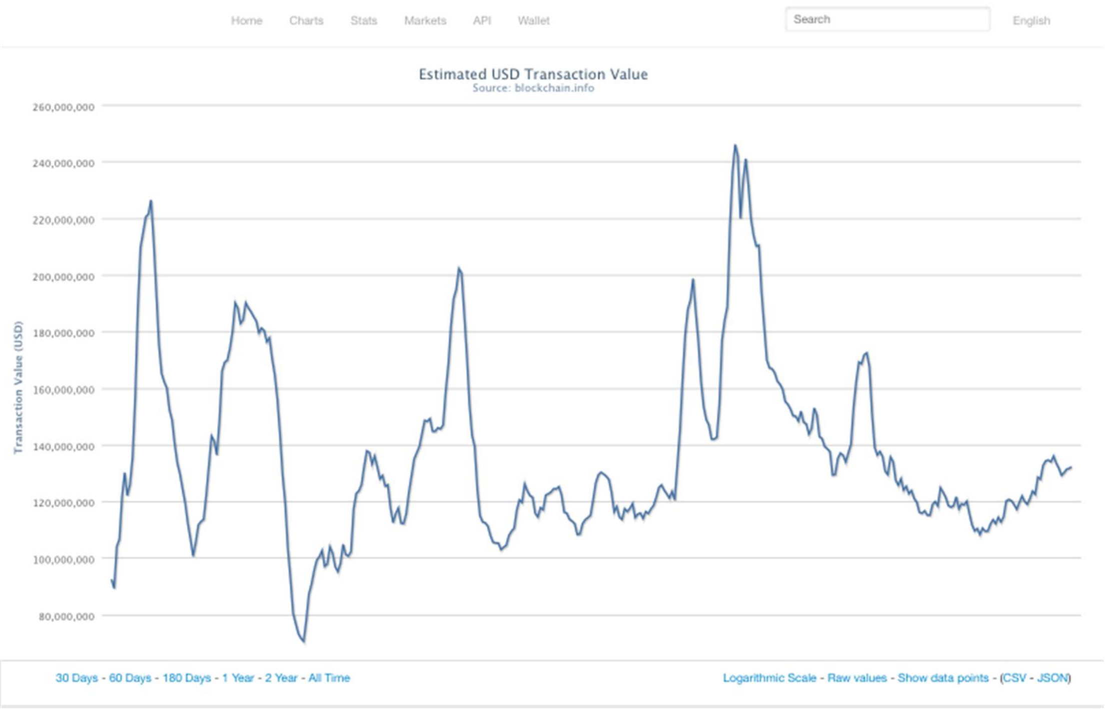

Fig. 1 Estimated daily USD transaction value of bitcoin blockchain

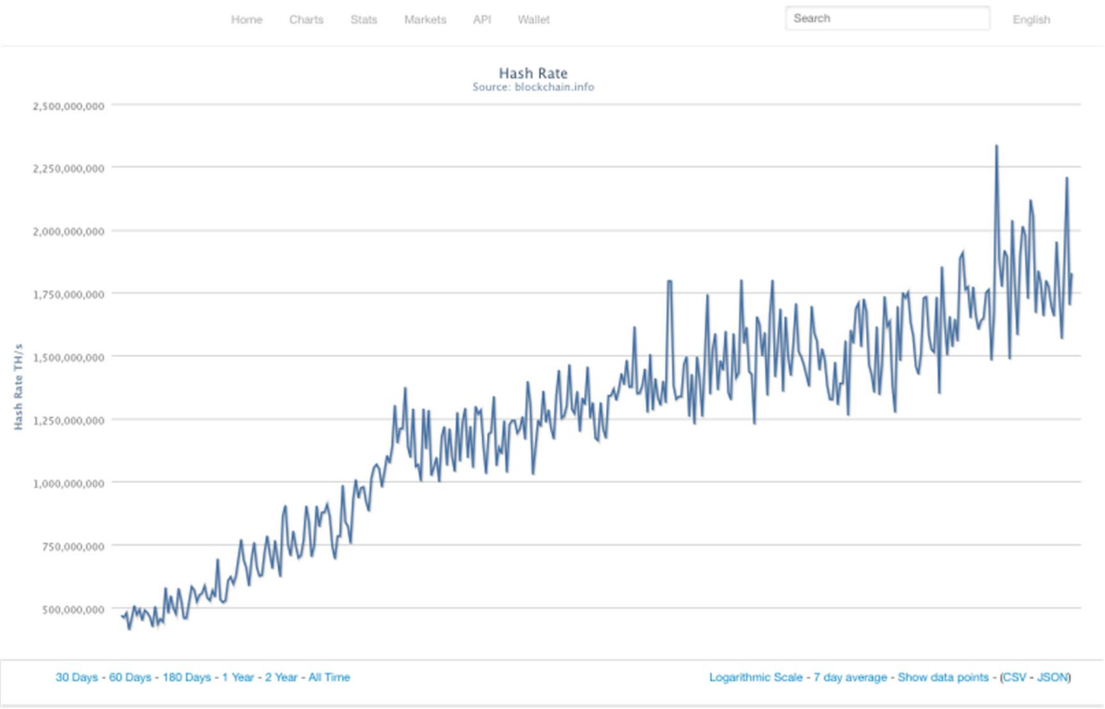

Fig. 2 Hash rate of bitcoin network

Currently, solo miner is very difficult to get rewarded. Mining pools are more likely to get rewards. Solo miner can join a mining pool to share the rewards and diversify his/her risk. Fig. 3 shows the major mining pools and their computing power.

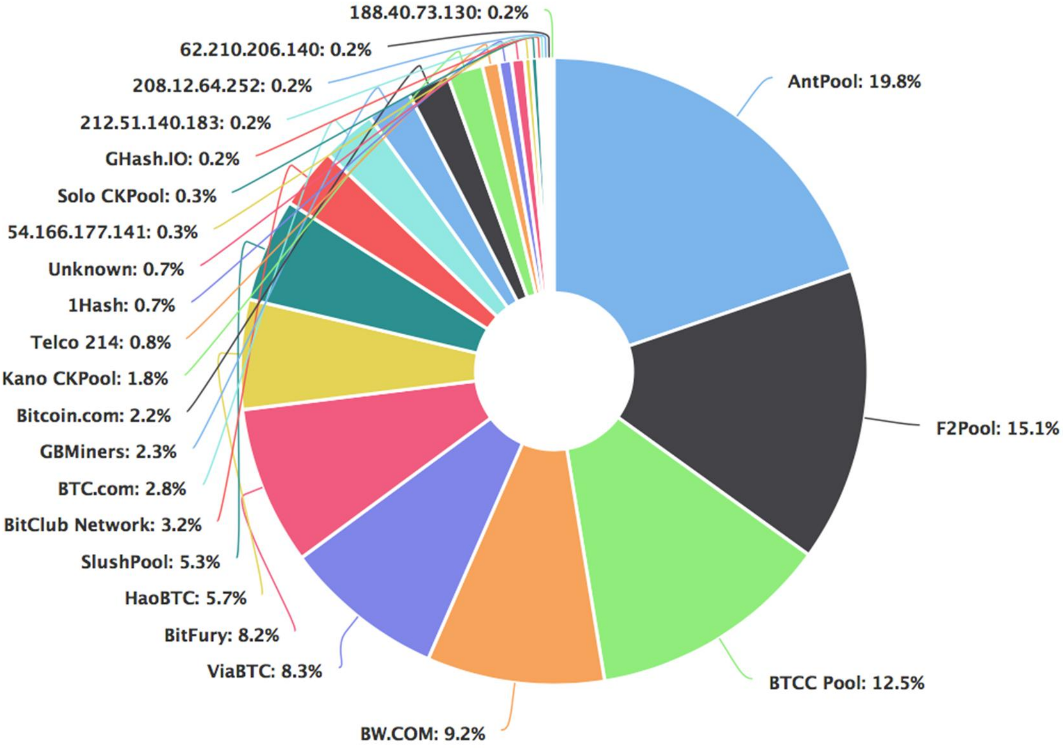

Fig. 3 Major mining pools of bitcoin network

ATTACKERS' MODEL

.

The basic attacker setup in [6] is as follows: "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". In this paper, we extend the analysis by adding more detailed assumptions. We assume two types of nodes: honest and attacker's. When an attack starts, it will last for N blocks. N can be deterministic or following a discrete random variable such as a Poison random variable. Assume attacker's node control w of total hash power when the attack begins. During the attacking period, an attacker's node will remain as an attacker's node with probability α when a block is created; and an honest node will remain as a honest node with probability β when a block is created. Based on these model assumptions, the majority decision is a two-state stochastic process (Asmussen and Glynn (2007)). More precisely, let $X_0, X_1, X_2, \ldots., X_N$ denote the random outcomes of the created blocks. We assume $X_1 = 1$ if it is created by an attacker's node and $X_1 = 0$ if it is created by an honest node. It is clear that

$$P(X_0 = 1) = w$$

$$P(X_1 = 1) = \alpha w + (1-\beta)(1-w) \equiv \mu_1$$

It can be shown that

$$P(X_n = 1) = \alpha\mu_{n-1} + (1-\beta)(1-\mu_{n-1}) \equiv \mu_n$$

for *n = 2, ... N*. From above recursion, we can also compute

$$P(X_n = 1) = 1 - \beta - [(1-w)(1-\beta) - w(1-\alpha)](\alpha + \beta - 1)^n$$

for all n.

Since only the double spending attack can incur loss, we assume the random loss L_n is incurred when block n is created by a hacked node or $X_n = 1$. The total loss of such an attack is

$$L = \sum_{n=0}^{N} L_n \, I(X_n = 1)$$

From the states of the majority decision, all of the interested quantities can be derived via simulation. The interested quantities are *EL* and risk measures of *L*. To estimate such quantities via simulation, computational efficiency is usually an important and practical issue. Fast simulation algorithm for similar network problem can be found in [1] and [3] and fast simulation in financial applications can be found in [2], [4], [5].

CONCLUSIONS

We proposed a probability model to address the importance attacker's issue in standard blockchain protocol. Based on model's parameters, we are able to address the probability of the system of being hacked in a certain time point. Furthermore, we are able to compute the expected loss and extreme loss during an attack event.

REFERENCES

[1]. Asmussen, S., Glynn, P. Stochastic Simulation: Algorithms and Analysis: Springer 2007.

[2]. Chiang, M.-H., Yueh, M.-L., Hsieh, M.-H. "An efficient algorithm for basket default swap valuation." The Journal of Derivatives, 15, 2 (2007), pp. 8-19.

[3]. Heidelberger, P. "Fast simulation of rare events in queueing and reliability models." ACM Trans. Model. Comput. Simul., 5, 1 (1995), pp. 43-85.

[4]. Hsieh, Ming-Hua Liao, Wei-Cheng Chen, Chuen-Lung (2014). A Fast Monte Carlo Algorithm for Estimating

Value at Risk and Expected Shortfall. *The Journal of Derivatives*, 22(2),50-66.

[5]. Glasserman, P. Monte Carlo Methods in Financial Engineering. Springer Verlag, New York, 2004.

[6]. S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. (2012): 28, 2008.