2018 5th International Conference on Dependable Systems and Their Applications (DSA)

Analysis of Security in Blockchain: Case Study in 51%-Attack Detecting

Congcong Ye[*], Guoqiang Li[*]✉, Hongming cai[*], Yonggen Gu[†], Akira Fukuda[‡]
[*]School of Software, Shanghai Jiao Tong University, Shanghai, China
{yecongcong, li.g, hmcai}@sjtu.edu.cn
[†]School of Information Engineering, Huzhou University, Zhejiang, China
gyg@zjhu.edu.cn
[‡] Kyushu University, Fukuoka, Japan
fukuda@f.ait.kyushu-u.ac.jp

***Abstract*—Recently, the global outbreak of a blackmail virus WannaCry, makes the blockchain a hot topic. The security of blockchain is always the focus of people's attention, and it is also the main reason why the blockchain has not been widely used all over the world. Many researches use mathematical derivation method to analyse the 51%-Attacks influence of blockchain, which is very stiff and difficult to understand. In this paper, we propose a method to simulate blockchain's process and discover the rule between attacking method, attacking power and security of blockchain. We take 51%-Attacks as an example and use Java to simulate the running process. By adjusting the value of attacking power, we can get most states of blockchain and analyze the probability that honest state becomes attacking state. We use various forms to analyze and show the experimental result, which verify our method is correct and feasible. This method can also be implemented as a middleware software of blockchain to detect the security of blockchain.**

I. Introduction

Decentralized cryptocurrencies like Bitcoin have captured the public's interest, and have been much more successful than any prior incarnations of electronic cash [1]. Bitcoin uses a data structure known as blockchain to store the transactions. Blocks, which are batches of updates to the log, reference the parent they are extending, and thus form the structure of a chain[2]. The blockchain technology provides a decentralized, open, Byzantine fault-tolerant transaction mechanism, and promises to become the infrastructure for a new generation of Internet interaction, including anonymous online payments, remittance, and transaction of digital assets [3]. Blockchain is the basic technology of bitcoin, which proves to be more valuable than the currency it supports. When we start to put this technology in use, it is very important to make sure its security.

Actually, there are many kinds of attacks in blockchain such as 51%-Attack, eclipse attack, physical attack and so on. Many researches use mathematical methods to analyze the impact of attacks in order to evaluate the security of blockchain. Heilman et al[4]. use a detail mathematical method to analyze the affect of eclipse attacks. And he also use a similar method to implement, evaluate and detect a double-spending attack on bitcoin. But the attacks in blockchain have not been fully identified yet and there are still many people searching for the new attacks in blockchain. So analyzing the effect of each attack in blockchain is incomplete and there is an intense need to evaluate the security of blockchain completely.

To address the aforementioned challenges, a method is proposed to analyze and evaluate the security of the blockchain. We construct a model to represent the process of blockchain, in which 51%-Attack is the only attacking method, using two kinds of algorithms to simulate honest miners and attackers. By running the simulation process, we record the honest state number and attacking state number in different conditions. The result of experiments can be used to evaluate the security of blockchain. We regard the attacking states as target, and calculate the probability that each state becomes attacking state. If this probability reaches a high value, we can send a warning to all users in blockchian to defend being attacked. Meanwhile

978-1-5386-9266-0/18/$31.00 ©2018 IEEE
DOI 10.1109/DSA.2018.00015

we use various methods to show our experiment and analysis.

According to the relevant researches, when a block connects with enough blocks, the message stored in this block can hardly be reversed and we regard this state as stable state. If this block contains illusory transactions, it is called as attacking state, or it is security state. In practical application, if more than six blocks are connected to a block, this block will almost be stable state and we do not need to process it any more. All these phenomenons indicate the states of blockchain are limited. If we can get most states of blockchain, the security of blockchain can be evaluated by analyzing the probability that each state of blockchain becomes attacking state. Our main contributions are summarized as follows:

- A simulation model is proposed to evaluate the security of blockchain. We take the 51%-Attack for an example and implement this simulating model by Java. From this program, we get most states of blockchain including the attacking states, which validates our speculation that the states of blockchain are limited.
- The relationships between attacking power and state number are revealed by some simulation experiments.

The rest of this paper is organized as follows. Section 2 discusses the related work in this field. Section 3 introduces the basic concepts, and some essential parts in blockchain. Section 4 presents the detailed definitions of honest miner and attackers in blockchain. Section 5 proposes a novel method to solve these problems. Section 6 evaluates this approach with several experiments and analyzes the experimental result. Section 7 concludes the work in this paper and illustrates the future direction of this work.

II. Related Work

Blockchain ensures the elimination of double spending in bitcoin which is a peer-to-peer electronic cash system. On the surface, comparing blockchain to banking systems, decentralised systems can better protect themselves against attacks, and route around damage. But there are still many attacks happening in blockchain and causing great damages to the users' security.

DDos attack is very common in blockchain system. Vasek et al[5]. present an empirical investigation into the prevalence and impact of distribute denial-of-service(DDos) attacks on operators in the bitcoin economy. They find currency exchanges, mining pools, gambling operators are much likely to be attacked than other services. And the big mining pools are much likely to be DDosed than small pools. Danny[6] introduces and analyzes the problem of bitcoin including 51%-Attack, double-spending, dust transactions and code-based attacks. These attacks all make it possible to manipulate the network for personal gain. Herrmann et al.[7] evaluate the potential of double spending attacks on bitcoin and analyze the bitcoin system, in particular the double spend protection procedure, and identify a weakness in certain usage scenarios. As many attacks being found, people expect to analyze the features in order to solve or defend them. Decker et al.[8] analyze how bitcoin uses a multi-hop broadcast to propagate transactions and blocks through the network to update the ledger replicas. All these researches on blockchain are very important and useful to improve its security.

With the development of blockchain, there are many applications based on it. Watanabe et al.[9] propose a new mechanism to secure a blockchain applied to contract management such as digital rights management. Digital contracts can decrease users' fees and make it impossible for anyone to change or deny the content. Based on the imbalances caused by asymmetric information and opaque supply chains, Badzar el at.[10] aim to contribute to the research field of logistics and supply chain management by exploring the potential of blockchain technology within logistics. They use blockchain to increase supply chain transparency for both suppliers and consumers, which will improve the security and normalization of shopping online. Wilkinson et al.[11] create an open source software project seeking to prove conceptually that cloud storage applications can be made more decentralized, more secure, and efficient. Even some people use blockchain as a software connector. Xu et al.[12] propose a new method that new forms of distributed software architectures can find agreements on their shared states without trusting a central integration point or any particular participating components. Using blockchain technology in software engineering, it will make software developing process more standard and improve the success rate of developing software.

According to Alibaba's outlook about ten top technologies in the future, the blockchain is regarded as a great potential and meaningful technology. Hence it is necessary for us to do more researches on blockchain.

III. Preliminary

In this section, we introduce some basic concepts of blockchain including the definitions of blockchain, mining process, Nakamoto consensus and some common attacks.

A. Blockchain and Mining

Blockchain represents a novel application of cryptography and information technology to age-old problems of financial record-keeping, and they may lead to far reaching changes in corporate governance[13]. It can be used to record the transactions in bitcoin. Each block in blockchian consists of a unique ID, the ID of former block, transactions, time stamp and so on, which are parts of the protocol. A valid block contains a solution to an encryption puzzle and the bitcoin address which is to be credited with a reward for solving the encryption puzzle[14].

The most important and famous process of blockchain is mining. Miners are always collecting the transactions which are created in a period of time. Then the miners will use the Hash256 algorithm to process these transactions and get a string, which must start with some zero and the number of zero must be more than the threshold value. If not, the miners have to repeat the mining process. The blockchain system has set the threshold value to represent the difficulty of the problem. And this value is dynamically adjusted every ten minutes. The larger the threshold value is, the more operations have to be done. When the string fits for the requirement, the miners will be rewarded a certain number of bitcoin that did not exist before. This process is similar to the bank to issue money.

After processing the block successfully, the miners will publish it over the network and other miners will validate whether these transactions and the mining string are correct. If two blocks have the same former block, the blockchain will create a fork. After that, miners can add a new block to any branch. In order to keep unanimous, the blockchain protocol stipulates that only transactions in the longest chain will be accepted and others will be ignored. Miners would better mine the new block after the longest chain. With this protocol, the blockchain is consistent and every miner will have the same structure. Only in a very short interval, the blockchain will be different, which is the main reason why attacks can occur in the blockchain. In real conditions, the average mining interval is ten minutes. Therefore accidental bifurcation is rare, and occurs on average once about every 60 blocks[8]. Attackers use this property to reverse the transactions. In order to solve these challenges, the Nakamoto consensus method is proposed, which is a mathematical method to solve the problem of trust.

B. Nakamoto Consensus

The most important feature of blockchain is a set of protocols, which are called Nakamoto consensus. It can solve the problem of trust without a center organization. In theory, there is not a robust method to ensure consensus, any participant could, for example, spend the same bitcoins multiple times (known as the double-spend problem), or claim it had more currency than it really did[15]. The Byzantine fault tolerant protocol can be used to solve this problem, which is similar to the voting process. In blockchain, every node can read all transactions and collect new transactions which have more fee or other features. After mining a new block successfully and broadcast the new block to other nodes, other nodes will validate this block and decide whether connect this new block to the branch or not. Everyone can join blockchain and express their opinion. Hence if the voting process is so easy for participants, all transactions including illusory transactions also can be recorded in the blockchain, which makes the blockchain losing credible feature and becoming unsafe.

Proof-of-work algorithm is proposed to solve this challenge, which is like academic certificate. Proof-of-work requires expensive computing hardware and particular machine. If a miner finishes proof-of-work, it represents this miner may not be an attacker, or an attacker has to spend more time attacking the blockchain. The correctness of blockchain, so long as over a half of the network's power are honest, will be believable.

C. Attacks and State

In this section, we introduce some famous attacks such as eclipse attacks, selfish miner attacks and 51%-Attack. At the same time, we introduce the state including attacking state, honest state and security state.

In the blockchain, miners only broadcast the newest block to their neighbors rather than all nodes, which causes potential danger of blockchain. If the attacker monopolizes all of the victims incoming and outgoing connections, it will isolate the victim from the rest of its peers in the network[4]. Especially, this isolated block is the key node for some blocks, and all messages have to be transmitted through it. When this block's incoming and outgoing connections are occupied, it forces the honest miners to waste computing power on obsolete views and use their computing power for attackers' nefarious purposes. For example, the attackers can send request to the key node to occupy their connections. The main challenge of eclipse attack is to obtain a sufficient number of IP address. This attacking process is called eclipse attack.

Selfish mining[16] is a well-known attack where a selfish miner, under certain conditions, can gain a disproportionate share of reward[1]. An attacker can keep some discoverable blocks private until the number is large enough. When the public branch approaches the length of private blocks, the attackers will broadcast these blocks, which will make both attackers and honest miners waste power. But the honest miners will waste more power, and attackers will get competitive advantage. There are various attacks in blockchain, and each of them has different feature and effect. All of these make it difficult for us to detect or divide them.

State represents a storage structure of blockchain including the number of branches, type of every nodes. State consists of honest state and attacking state. Attacking state is the structure that a node contains illusory transactions and connect with more than six nodes. Transactions in this node could not be changed any more. Other structures are called honest state. Cycle is an important process in our experiment. When one node connects with many nodes and the depth of this structure is more than six, this structure will be cut off and restructured, which is a cycle.

IV. Problem Definition

The security of blockchain is always the focus of our attention, which will be affected by many kinds of factors such as the types of attacks, state of network,progress in science and so on. In this section, We propose the formal representation of 51%-Attack, honest miner, attacker and the protocol of blockchain.

A. 51%-Attack Representation

One of the most famous attacking method in blockchain is 51%-Attack[17], which is hypothesized that a group of miners control more than 50% of the network's mining hashrate, or computing power. The attackers would be able to prevent new transactions from gaining confirmations, halting them between merchants and clients. Attackers can complete proof-of-work quicker than honest miners. As a result, their transactions will be connected to the longest chain. The more mining hashrate they control, the faster attacks happen in blockchain. 51%-Attack can be used to reverse transactions and spend same coins many times when attackers control more than 50% network's mining hashrate. Satoshi Nakamoto[18] proposed the framework of bitcoin and calculated the attacking probability on different computing power that attackers controlled. The speed of honest chain and attacking chain is characterized as a binomial random walk. The rate that an attack can catch up with the honest chain is presented as follows[8]:

$$q_z = \begin{cases} 1 & p \leq q \\ (q/p)^z & p > q \end{cases} \tag{1}$$

p represents the probability that honest nodes find the new block first, q is the probability that attackers mine the new block faster than honest miners and q_z is the probability attackers catch up honest nodes from z blocks behind.

In probability aspect, if attacking power is larger than the honest power, the attackers are certain to catch up with the honest chain successfully. Actually, the probability of attacking is effected by many factors such as the change of the network's mining power, the difficulty of proof-of-work and so on. In this paper, we simulate the whole process of blockchain and count most states of blockchain. Then we can calculate the security probability of blockchain by analyzing every state. In order to know more details about the process of blockchain, we use formulas to represent the protocol of blockchain from the aspects of honest miner and attacker.

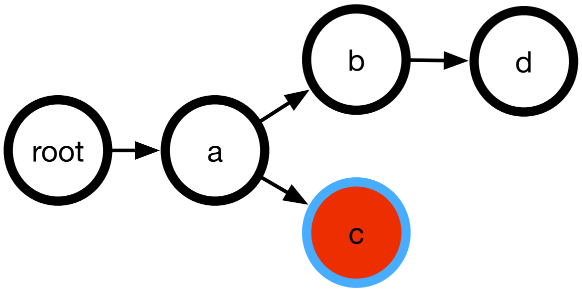

Fig. 1. A case on attackers' strategy

B. Attacking Strategy Representation

Blockchain is a decentralized system. Everyone including attackers are able to join and maintain it. People who want to reverse the transactions and spend the same bitcoin more than one time are called attackers. The type of each block is unknowable for honest miners, but attackers are clear whether the blocks contains illusory transactions or not. Attackers can connect the newest illusory block to the most suitable one, which will speed the process of attacking. The selection strategy is defined as follow:

$$R = \begin{cases} max \sum\limits_{v_i \in U_{attack}} child(V_i) & \sum\limits_{i=1}^{n} child(V_i) \geq 1 \\ max \sum\limits_{v_i \in U_{all}} child(V_i) & \sum\limits_{i=1}^{n} child(V_i) = 0 \end{cases} \tag{2}$$

R represents the most suitable block the attackers will choose. V_i represents block i in attacking collection or in the whole blockchain. The $child()$ is a function to judge whether block V_i has a child node. If there are no attacking nodes in blockchain, the attackers will choose the longest chain of blockchain. If not, attackers will choose the chain in which the attacking node connects with most nodes.

The figure 1 is a case of blockchain from the attackers' point of view. The red nodes represent the blocks which contain illusory transactions. The white nodes are the valid blocks. The blue border shows this block will be chosen. In this case, the newest node will connect red node c rather than node d or others. Attackers expect more and more nodes can be connected with their own node, which will make their node in the longest chain. Meanwhile, their transactions will be more safer if more nodes connect with their node. According to Satoshi Nakamoto[18], it is obvious that the more blocks connect with a block, the safer the block is. Many researches show that if more than 6 blocks are connected to a block, the message in this block could not be changed any more in real conditions. After more than 6 blocks are connected to an illusory block, we can regard that this blockchain has been attacked successfully. So the attackers will connect the newest block to the longest chain in order to add the probability of attacking, which is the most common attacking strategy. In this paper, we use 51%-Attack as the only attacking method. It doesn't matter which attacking strategy is used, and the total state of blockchain will not change. Only the probability that an honest state becomes attacking state will change when the attacking methods are different.

C. Honest Miner Representation

As for honest miners, the types of blocks are unknowable. In blockchain system, only the transactions in the longest chain are regarded as the correct records. Hence the honest miners incline to connect their newest mining block to the longest leaf node. If there are some leaf nodes having the same depth, the honest miners will choose them at the same rate. According to this principle, we can use simple method to simulate the honest miners. If the depth drops one layer, the probability will be halved. We can use formula (3) to calculate the probability that the nodes in the longest layer will be chose. From formula (4) we can get the probability that the node p_{ij} will be selected.

$$\sum_{i=1}^{n}\sum_{j=1}^{m}\frac{1}{2}^{(L-i)}P = 1\ . \tag{3}$$

$$p_{ij} = (\frac{1}{2})^{L-i}P\ . \tag{4}$$

L is the depth of whole blockchain. Based on the different state of blockchain, the threshold value P will change. i represents the layer number and j is the order number in layers. Actually, the probability that honest miners choose the block in former layer rather than the longest one is lower than the value we set in our model.

In this paper we expect to get the whole state of blockchain system, which is more stable than the types of attacks. The total states of blockchain have no relationship with the decreasing rate. In simulation model, it is feasible to set decreasing rate of honest miners as 0.5. Honest miners' strategy is more complex than the attackers' algorithm. Because honest miners can not recognize which block contains illusory transactions, and all blocks are the same to them. According to Nakamoto Consensus[18], honest miners incline to validate and broadcast the newest blocks of which former blocks are connected with the longest chain. But it is feasible for them to choose others.

V. Methodology

In this section, we introduce the simulation methods of blockchain system, attackers and honest miners. We use a mathematical method to prove that the state number in blockchain is limited.

A. Solution Overview

Blockchain is a large and complex decentralized system which uses mathematical approach to solve the trust problem between two sides. So it is regarded as a significative technology and has the best prospect. In this paper, we use another method to assess the security of blockchian. We construct a simple model of blochchain and describe the blockchain's action from honest miner and attacker point of view. We count all states of blockchain system by simulation process and analyze the probability that honest states become attacking state in order to assess the security of blockchain.

B. Simulation Process

Firstly, we research the protocol of blockchain with simplified condition, in which we ignore the detail of proof-of-work, quality of network and so on. We only use a tree structure to subscribe the blockchain and allocate every node a type which represents it is the honest block or attacking block. We set a threshold value to represent the computing power which is controlled by attackers and decides the probability that the newest block becomes attacking block. According the block's type, we will take different strategies to connect the newest node, which represents the mining and broadcasting process in blockchain.

Algorithm 1 Obtain all state of simulation process about blockchain

```
Input: The attacking power $P$
Output: All state of blockchain $S$
Initialize a blockchain with a honest node $R$
Create a new block based on network's attacking power;
repeat
    create a new block based on power of attacking P;
    if new block is honest one then
        Algorithm 2;
    else
        Choose the longest chain which will make attacking block more safer.
    end if
    Reconstruct a new tree by connect new block to the choosed node;
    if the state of new tree is different from the state in S then
        Join the new state into S
    end if
    if the new tree reaches security state or attacking state then
        Initial a blockchain with a honest node
    end if
until the state number of blockchain $S$ converges
return all state of simulation process about blockchain $S$
```

Algorithm 1 represents the simulation model, which ignores proof-of-work, digital signature, timestamp service and so on. Because these complex actions have no relationship with the total states of blockchain. While the protocol always allows a chain to be undone by a longer chain and the possibility of any block being reversed always exists. The probability of such an event decreases as time passes until it becomes infinitesimal. Once a node reaches the security state, it can be cut off in order to decrease the complexity of our problem. After cutting off the security state, the states of blockchain are finite and the blockchain can be regarded as a cycle process. A start node increases to a security state and then cut off this security state, all these process is regarded as a circulation. In every circulation, we will restructure the cutting-off state and compare it with the states in the collection S. Only when two tree structures have the same branches and every node is the same type, we can regard these two structures represent the same state. The number of state has no relationship with the attacking power, which will be verified later.

Proof: The states of blockchain are finite.

According to Satoshi Nakamoto[18], the probability that attackers could still catch up from z block behind is $\sum_{k=0}^{\infty} \frac{\leftthreetimes^k e^{-\leftthreetimes}}{k!} \begin{cases} (q/p)^{(z-k)} & if \quad k \leq z \\ 1 \quad if \quad k > z & \end{cases}$. And using this formula, Satoshi give us some cases that if attackers control 30% computing power and five blocks have been linked after it, the probability that attackers reverse transactions is less than 0.18. In real conditions, 30% computing power is very difficult, so the transactions in the block almost could not be reversed when this block connects with six blocks. All above illustrates that the depth of block is limited.

Based on the honest miner's strategy, we can explain why the number of branches in blockchain is finite. When a root node has only one child, the probability that the newest node connects to root node is $\frac{2}{3}$. Then the probability that next node still connects to root node is $\frac{2}{5}$. We can get the probability that a node has five child is less than 0.017. The probability that all branch in blockchain have more than five branches will be much less.Hence we can regard that the branches in blockchain are finite. According to simulation model, the state number is less than $\frac{a_n q - a_1}{q-1} = \frac{5^7 - 5}{5-1} = 19530$.

C. Attack and Honest Mining Process

Mining is an important process in blockchain. According to blockchain's protocol, an honest miner is inclined to accept the transactions in the longest chain as the credible records. However, if two blocks are discovered at the same time, the blockchain may occur fork. The next block will connect with any one of them at the same probability, even the next block can choose their former block. It is very difficult to distinguish honest miners and attackers. Honest miners can connect the newest node to any block of blockchain at different probability. We use algorithm 2 to simulate their actions. Actually, this process will be more complex and honest miners are not inclined to connect with the former nodes. In our algorithm, we set 0.5 as the decreasing probability to simulate this phenomenon.

As for attackers, they are clear about the type of every block and their purpose is more specific. They expect to connect as more nodes as possible to the longest chain which contains illusory transactions. If there are not illusory transactions in blockchain, they will choose the longest chain. Actually, they can use all kinds of attacks to reverse their transaction even physical attack. It is difficult to take care of all situations including various attacks, attacking power and so on. We only need to construct a simple model to simulate and analyze this process. In section 5.2, we prove that the state number in blockchain is finite. So it is useful and feasible to evaluate the security of blockchain by using simulation program to get most states of blockchain system and analyzing probability that honest state becomes attacking state.

Algorithm 2 How to choose one node the new honest node will connect

```
Input: The root of the blockchain $P$
Output: One node that new honest node will connect $S$
Calculate the depth of a tree $L$
for every layer i=0 to n do
    for ever node j=0 to m do
        Add weight of every node
    end for
end for
Choose one node based on the probability $P$ that was calculated above
return node $S$
```

VI. Experiments

This part uses various methods to show the experimental results and analyzes relationship between cycle times, state number, and attacking number. Meanwhile some real attacking case are showed to validate that our method is useful.

A. The State of Blockchain in Different Attacking Power

The entire experiments were performed on a machine with three 1.8GHZ Intel Xeon CPU, equipped with 40G memory, x86_64 Linux, Java 8. We use all kinds of attacking power from 10% to 60% to simulate the process of blockchain.

In section 5.2, we have proved that the most state number of blockchain was less than 19530. In our experiments, the process will continue running until the number of cycle is larger than 25000. The more cycle times we set, the more state values we will get. It will take long time and is almost irrealizable to get all states of blockchain. Getting most states of blockchain is enough for our experiments. Figure

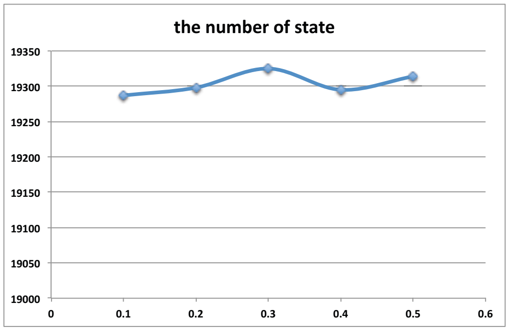

Fig. 2. The state number in different attacking power and large cycle times.

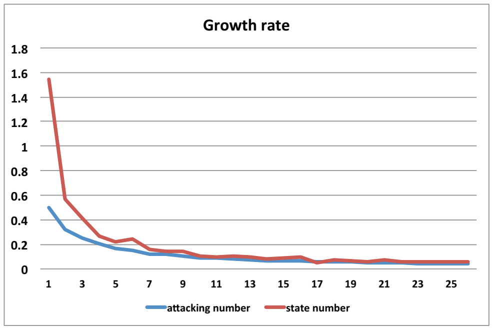

Fig. 3. The growth rate of state number and attacking number in different attacking power.

2 shows the state number in different attacking power when 25000 is set as cycle times. The max value in figure 2 is 19325, which is close to our estimated value 19530. Every state number in different attacking power is very similar and is about 19300. When attackers control 30% mining power, the state number becomes the highest value, which is nonsignificant for a random process. We only take care of the general trend. These results indicate that the total number of blockchain has no relationship with attacking power and it is a fixed value when the cycle times are large enough. This rule makes it possible to evaluate the security of blockchain by analyzing the probability that every state becomes attacking state. In the following experiments, we regard 19300 as the state number of blockchain system. We do some experiments to analyze the relationship between state number and cycle times. According to many researches, the blockchain can be regarded as being attacked successfully after six blocks are connected to one block which contains illusory transactions. Figure 3 shows the relationship between the state number and attacking number when cycle times change from 1000 to 27000. With the growth of cycle times, the state number and attacking number both increase. But the growth rate of them are different, the state number rises faster than attacking number.

When the cycle times are very small, the growth rate of state number decreases rapidly. When cycle times reaches 17000, the growth rate becomes smooth and almost remains unchanged. Because the limitations of experimental environment, we do not have more cycle operations. From the experimental result, we can infer that the growth rate will become lower gradually until zero when the process runs enough time. Then the state number will converge to a fixed value. The growth rate of attacking also decreases rapidly when the process cycles small times. With the continuous increase of cycle times, attacking number increases slowly, so as to achieve a stable value.

B. The Attacking Number in Different Attacking Power

The main purpose of this paper is to analyze attacking features and evaluate the security of each state. Hence we carried out more simulation experiments to analyze the relationship between attacking number and attacking power when the cycle time changes from 20000 to 26000 and attacking power changes from 0.1 to 0.6.

Figure 4 shows the result of these experiments. The abscissa represents different attacking power and the ordinate is attacking number. With the increase of attacking power, attacking number also becomes large gradually. It means that attacks will increase when attackers control more computing power of network, which is also in line with the reality. The different color lines represent different cycle times. We use the least square method to calculate the slope of these line. We find the slope becomes lower and lower with the increase of cycle times. From this picture we know that larger the cycle times are, more stable the attacking number becomes. Figure 5 shows the relationship between cycle times and attacking number. When the cycle time increases, the gap between max and min values become smaller and smaller. From these data, we can infer that the attacking number will reach a fixed value and the number of attacks are finite. At the same time, we find a special phenomenon about the state number and attacking number. Figure 5 shows the relationship between state number and attacking

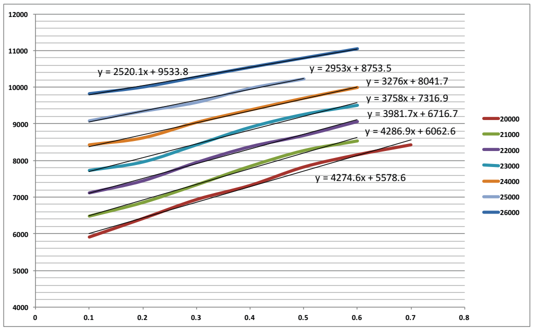

Fig. 4. The changed trend of attacking number in different attacking power and cycle times.

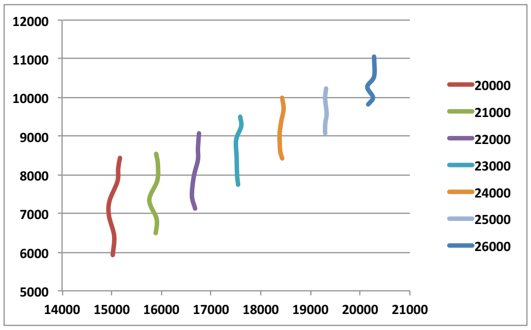

Fig. 5. The relationship between cycle times and attacking number.

number when cycle time is 24000 and attacking power changes from 0.1 to 0.6. The abscissa of this picture is attacking number and the ordinate is state number. The shape of this figure is similar to sine function. Then we change cycle time from 20000 to 25000, the figures we get are similar to figure 5. From these data, we know the relationship between attacking power and attacking number is not monotonous.

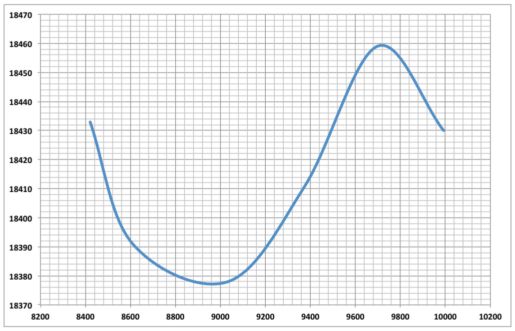

Fig. 6. The relationship between state number and attacking number in different attacking power.

C. Analyzing the Probability of Being Attacked Successfully

At last, we carry out some experiments to analyze the relationship between the depth of blockchain and state number. In these experiments, we set cycle time as 25000 and attacking power as 0.4. Then we get the total attacking number and state number, which are 8732 and 17356. So the percentage of attacking number in state number is about $8732/17356 \approx 0.5$. This result is up to our expectation. Because the honest strategy is a geometric sequence and the percent of state number in the sixth layer is about 0.5. Table 1 records the state number and the rate of each state number in different depth. We can find most of the states are in the sixth layer, and the percent reaches about 0.9. If the node is in the fifth layer, We can regard the nodes in fifth and sixth layer as connecting target and calculate the probability that the newest node connects with the nodes which belong to the fifth layer or sixth layer.

TABLE I
THE STATE NUMBER IN DIFFERENT DEPTH OF BLOCKCHAIN

depth	state number	proportion
1	1	0.000051843
2	15	0.000777645
3	113	0.005858261
4	871	0.04515527
5	6644	0.34444502
6	17356	0.899787444

By using simulation algorithm, we get most states including honest state and attacking state and analyze the probability of each honest state being attacked. We regard attacking state as the target and analyze the probability that each honest state becomes attacking state. The types of attacks have not be fully identified, and it is very difficult for us to detect them. But we can calculate the attacking probability of each state. If this probability is larger than a value we set, this method will send warnings to all people. And they can take some preventive measures to defend being attacked. If we can add a detecting tool in the blockchian and give us warnings based on the state of blockchain, it will make the system safer and more dependable.

VII. Conclusion

In this work, we propose a tree-structure method to simulate the process of blockchain and analyze the relationship between attacking number and state number in order to evaluate the security of each state. This method is generic and concise, and any attack in blockchain can use this method to analyze their influence by changing the attacking strategy. In this paper, we apply 51%-Attack strategy to simulate the attackers' behavior and obtain the change trend of state number and attacking number. After getting these data, we can evaluate the security of each state in blockchain.

The proposed method has some limitations. Firstly, we use the 51%-Attack strategy to simulate the process. We think the state number and attacking number have no relationship with the type of attacks, but we don't use more experiments to validate this conjecture. Secondly, we set regression rate that the honest miners choose the former block rather than the newest one as 0.5, which is only the experimental argument rather than real value. In the future, we plan to apply this method in real system to evaluate its security. Meanwhile, we will develop a more generic tool to detect the state of blockchain and send warnings to users that they could wait for a long time to accept the transactions, which will improve the security of blockchain.

Acknowledgements

This work is supported by the Key Program of National Natural Science Foundation of China with grant No. 61732013, and Key the R&D Project of Zhejiang Province with No. 2017C02036.

References

[1] K. Nayak, S. Kumar, A. Miller, and E. Shi, "Stubborn mining: Generalizing selfish mining and combining with an eclipse attack," in *Security and Privacy (EuroS&P), 2016 IEEE European Symposium on*. IEEE, 2016, pp. 305–320.

[2] Y. Lewenberg, Y. Sompolinsky, and A. Zohar, "Inclusive block chain protocols," in *International Conference on Financial Cryptography and Data Security*. Springer, 2015, pp. 528–547.

[3] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, "Bitcoin-ng: A scalable blockchain protocol," in *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*. USENIX Association, 2016, pp. 45–59.

[4] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, "Eclipse attacks on bitcoin's peer-to-peer network." in *USENIX Security*, 2015, pp. 129–144.

[5] M. Vasek, M. Thornton, and T. Moore, "Empirical analysis of denial-of-service attacks in the bitcoin ecosystem," in *International Conference on Financial Cryptography and Data Security*. Springer, 2014, pp. 57–71.

[6] D. Bradbury, "The problem with bitcoin," *Computer Fraud & Security*, vol. 2013, no. 11, pp. 5–8, 2013.

[7] M. Herrmann, "Implementation, evaluation and detection of a doublespend-attack on bitcoin," 2012.

[8] C. Decker and R. Wattenhofer, "Information propagation in the bitcoin network," in *Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference on*. IEEE, 2013, pp. 1–10.

[9] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. Kishigami, "Blockchain contract: Securing a blockchain applied to smart contracts," in *Consumer Electronics (ICCE), 2016 IEEE International Conference on*. IEEE, 2016, pp. 467–468.

[10] A. Badzar, "Blockchain for securing sustainable transport contracts and supply chain transparency-an explorative study of blockchain technology in logistics," 2016.

[11] S. Wilkinson, J. Lowry, and T. Boshevski, "Metadisk a blockchain-based decentralized file storage application," Technical Report. http://metadisk. org/metadisk. pdf, Tech. Rep., 2014.

[12] X. Xu, C. Pautasso, L. Zhu, V. Gramoli, A. Ponomarev, A. B. Tran, and S. Chen, "The blockchain as a software connector," in *Software Architecture (WICSA), 2016 13th Working IEEE/IFIP Conference on*. IEEE, 2016, pp. 182–191.

[13] D. Yermack, "Corporate governance and blockchains," *Review of Finance*, p. rfw074, 2017.

[14] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in *International Conference on Financial Cryptography and Data Security*. Springer, 2014, pp. 436–454.

[15] K. D. Werbach, "Trustless trust," *Browser Download This Paper*, 2016.

[16] A. M. Antonopoulos, *Mastering Bitcoin: unlocking digital cryptocurrencies*. " O'Reilly Media, Inc.", 2014.

[17] K. Kaskaloglu, "Near zero bitcoin transaction fees cannot last forever," in *The International Conference on Digital Security and Forensics (DigitalSec2014)*. The Society of Digital Information and Wireless Communication, 2014, pp. 91–99.

[18] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2009.