ISSN 0798 1015

REVISTA ESPACIOS

Vol. 41 (Issue 03) Year 2020. Page 29

Analysis of DDoS Attacks on Bitcoin Cryptocurrency Payment System

Análisis de Ataques DDoS en el Sistema de Pago de Criptomonedas Bitcoin

KOCHKAROV, Azret A. [1]; OSIPOVICH, Sergey D. [2] & KOCHKAROV, Rasul A. [3]

Received: 05/11/2019 • Approved: 14/01/2020 • Published 07/02/2020

Contents

ABSTRACT:
The work researches DDOS attacks on the Bitcoin cryptocurrency system, describes its basics, mechanics of attacking algorithms and results of such attacks. For the purposes of researching and modelling possible consequences, the research suggests using the DDOS attack detection technique, based on creating a directed transaction sequence graph and identifying statistical deviations. In order to do so, the components of low graph connectivity are researched and a special attack-registering index are calculated.
Keywords: Cryptocurrency System, Blockchain, Bitcoin, DDOS Attack

RESUMEN:
El trabajo investiga los ataques DDOS en el sistema de criptomonedas Bitcoin, describe sus conceptos básicos, la mecánica de los algoritmos de ataque y los resultados de tales ataques. Con el propósito de investigar y modelar posibles consecuencias, la investigación sugiere usar la técnica de detección de ataque DDOS, basada en la creación de un gráfico de secuencia de transacción dirigida e identificación de desviaciones estadísticas. Para hacerlo, se investigan los componentes de la conectividad de gráficos bajos y se calcula un índice especial de registro de ataques.
Palabras clave: Sistema de criptomonedas, Blockchain, Bitcoin, DDOS Attack

1. Introduction

The first and the most renowned case of Blockchain Technology (decentralized peer-to-peer database) is the Bitcoin cryptocurrency. Such type of currency uses the solution of complex cryptographic problems as its PoW (proof-of-work). A number of various cryptocurrencies are currently being offered at the digital stock exchange market [4] with 10-15 of them being specifically recognized and trusted by customers, such as Bitcoin, Ethereum, Litecoin, Monero, Peercoin. Cryptocurrency market capitalization exceeded $172 billion [5] by the end of December 2019, with Bitcoin estimated as $45 billion, and Ethereum – as $17 billion [9, 3, 11].

Another way of using the Blockchain Technology is for smart contracts. The concept of smart contracts implies automating fulfillment of contract terms (liabilities, confidentiality, property rights etc.) by using a certain environment (software and hardware) that describes these terms in a mathematically correct way. As frequently used, an example of it is the digital car safety system. Smart contract presumes that the control over car control crypto keys (i.e. safety system, alarm system) belongs to the owner in accordance with the contract terms. The car can’t be controlled until the owner authentication protocol is completed. The best example of it in the modern world is the car sharing service that includes not only car usage payments but also insurance payments and punitive penalties for breaking the terms of the smart contract (the contract signed in a smartphone app). The practical application of smart contracts has become possible due to blockchain technologies. Some features of smart contracts are implemented at the cryptocurrency market (for example, in Ethereum [6, 5, 1]).

Smart contracts will indeed become widely used due to the mainstream digitalization in people's life. It was announced that smart contracts are planned to be used in configuring Russian Registry records, payment (transaction) processing in Sberbank, creating digital personal employment books, running various social questionnaires, including those in social media. Social profiles already require the information to be validated by several users before it is deemed reliable [2].

The objective of the study is to identify DDos attacks based on historical data (formed blocks) and analyze the consequences of such attacks. DDos attacks can completely paralyze the cryptocurrency system, i.e. stop cryptocurrency circulation or block processing for a while. Stopping the system can be used for a short-term reduction in the cost of cryptocurrency, or for other fraudulent activities.

To analyze historical data, it is assumed that transactional movements are simulated using graphs.

2. Blockchain Technologies and Attacks on Cryptocurrency Systems

Blockchain is the technology built on creating and exchanging consecutive information-containing blocks between network peers. For cryptocurrency it is a sequence of blocks that contain transaction data. It can be said that blockchain is a distributed calculation technology that inputs data in the equally distributed database. The database contains information on all actions (transactions), while its copies are stored at numerous computing devices (computers, servers etc.) included in the data processing system. Information in the blocks in not encrypted and openly available, its integrity is confirmed by cryptographic hashing functions. The main difference between various cryptocurrencies is the hashing algorithm, most popular algorithms being SHA-256, Ethash, Scrypt and their variations [12, 10].

DDOS attack is the abbreviation for Distributed Denial of Service. Such type of attack is used to create service malfunctioning, even a complete shutdown. The attack is called "Distributed" as it is delivered by a computer network. For cryptocurrency systems, such attack may target transaction processes, instantly increasing the number of transactions processed and thus inhibiting generation of new ones. DDOS attack is a rather costly operation, as transaction fees depend on the amount of currency transferred and on the volume of generated data – and it is worth mentioning that transactions with the highest fees are validated first. Despite this fact, the profit of potential system slowdown or shutdown is notably higher than expenses on fake transactions. For example, in summer 2017 an alleged DDOS attack targeted the Bitcoin cryptocurrency system, resulting in performance slowdown. One of explanations for this attack was the promotion of a new derivative currency, Bitcoin Cash. Unfortunately, such attacks, in addition to the visible damage, also leave consequences in the form of increased data storage and processing volume. As the blockchain technology doesn't imply deleting (changing) sequences, false transaction are stored in the system and participate in further calculations.

The flipside of cryptocurrency system appeal for financial operations is the increased number of cases when they are used in violators' interests. Abusive practices are frequently accompanied by actions intended to hide financial operations (transactions) or bust up the performance of the cryptocurrency system itself. It is usually done with computer attacks. Creating methodology that allows to detect attacks is an important scientific and practical task. To create such technique, it is assumed that indirect signs are used that would signal an attack or a new one. As mentioned earlier, for a qualitative analysis, it is necessary to build a model of the transaction structure of the studied cryptocurrency.

One of the easy-to-organize attacks on the Bitcoin cryptocurrency system, in experts' opinion, is the DDOS attack. It results in slowing down the system by creating numerous transactions to transfer assets through and forth between the attacker's pre-created wallets. The slowdown is caused by the need to process all transactions, i.e. it takes more time to process ongoing transactions executed by decent Bitcoin customers. In its turn, it hinders turnaround time for the next block (cryptoblock), the operating basis for the whole cryptocurrency system. The cryptocurrency system itself counterposes such attacks with transfer fees, sometimes higher than the transferred asset volume (it is logical for violators to transfer small amounts, as the attack should be executed at a least cost) [8, 13].

The information about the most popular cryptocurrency systems (blocks in particular) in accordance with their operating logic is freely available at https://www.blockchain.com. Blocks contain transaction data for a specific period.

3. Modelling the Cryptocurrency System

After we specify the block for analysis, the transaction sequence can be represented as an oriented graph, as follows:

1. Specify two peak types: those that represent transactions and those that represent Bitcoin wallet addresses.

2. Draw directed lines from input wallet peaks to the transaction peak, and from the transaction peak to the peaks that signify output wallets – transfer destinations.

Let's implement designators for the graph or any of its connected components: *V*, *N*, *E* – sets of destination peaks, transaction peaks and ribs, so *V_a* is the average transaction value, Δt – the transaction sequence period. It is clear that the transaction sequence graph is dynamic and evolutionary [4], in accordance with the real transaction validation time.

The methodology for identifying DDOS attacks that target cryptocurrency systems is applied in stages.

Stage 1.Identify low-connected components of the graph, then remove low-connected components that contain less than n transactions. The number of transactions in n should be specified with expert analysis tools. For the purposes of this study $n = 10$.

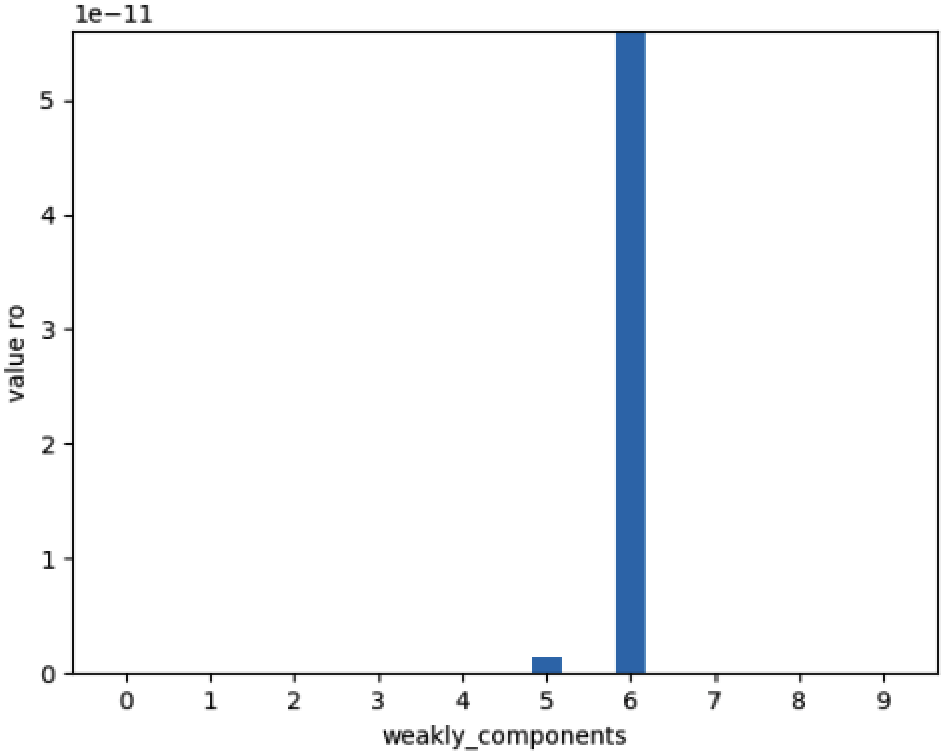
Note 1.As each block usually contains 1-3 thousand transactions, it is counterproductive to analyze all connected components in such a large-scale graph. The average number of transactions in low-connected components for 10 blocks adjacent to the one analyzed, is equal to 2.85.

Stage 2. Calculate the index $f = \frac{|E|}{\Delta t * V\_a}$ for the remaining graph components.

Note 2. The index f is the most informative for studying designated transaction sequences. Using graph density in its classic meaning $\rho = \frac{|E|}{N^V + V^N}$ as such doesn't let us clearly identify the transaction sequences in question. Graph 2, shows that the highest value is attributed to the connected component with 12 addresses and 10 transactions, which doesn't correspond the characteristics of a cryptocurrency system attack.

Graph 1

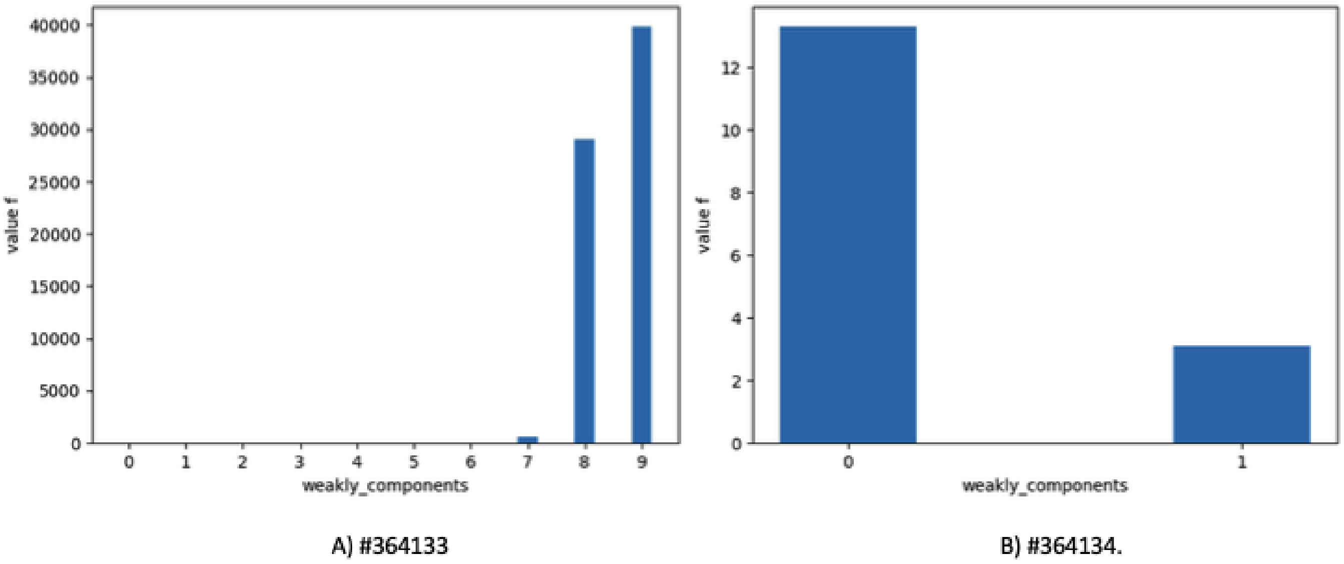
Index $^{\rho}$ value for block #364133 (author's calculation)



In accordance with the logical structure of the attack type in question[9], the index *f* allows us to estimate changes in graph density in the course of time, i.e. the ratio of the number of transactions to the time period of their execution, with regard to their average value.

Graph 2, shows the results of the DDOS attack detection technique through the cases of two different blocks, #364133 and #364134. Comparing pic. 2 A and pic. 2 B, we can see the difference in the index *f* value (the scale should be also taken in consideration) for attacked and non-attacked blocks. Looking at the block #364133, we can suppose that the attack was executed by two parties, *V_a* in each of two components with the highest value of *f* are equal to 0.157 BTC and 0.077 BTC (43,2$ and 21,2$ by 2015-07-06) accordingly.

Graph 2
Index *f* values for transaction
blocks (author's calculation)



A) #364133

B) #364134.

4. Conclusions

It has to be noted that from a practical perspective the calculation of the index *f* value in a real-time environment, while creating transaction blocks, can be used as a protection from DDOS attacks, allowing to block the wallets that participate in malicious transactions without increasing transaction fees for decent Bitcoin cryptocurrency system users.

Blockchain technology has an important feature – increasing complexity of calculations for each new block. On one hand, it is a weakness of this technology, as each new transaction requires more and more operations, and on the other hand, it is extremely difficult to execute false transactions as they will require the calculations to be finished faster that the rest of the network, using at least 50% of all capacities.

Vast number of transactions and complexity of cryptocurrency systems allow violators to find new openings for attacks in order to block the system (shut it down) or commit other unlawful acts [7].

The next stage of research in this field implies visualization of transaction graphs and attack signs, statistical check of the offered density index, comparison with classic graph index values, classification of transaction graphs (dynamic, self-similar, big and other classes), analysis of graph properties in the selected class.

From a practical point of view, the authors intend to visualize the transactions of the Bitcoin cryptocurrency system, and compare the signs of attack with the calculated data with the transaction graph. Determining the amount of cryptocurrency involved in fraudulent activities, including determining the amount of cryptocurrency used in DDOS attack.

This study was conducted with the support from the Russian Foundation for Basic Research (project № 19-01-00602).

Bibliographic references

Artamonov, V.A.; Artamonova, E.V. (2019) Application of Semantic Technologies and Blockchain in the Legal Field. *Zaschita Informatsii. Insaid [Information protection. Inside].* 2, 25-33.

Guria, D.G.; Mitin N.A. (February 8-9, 2018) Blockchain and Cryptocurrencies: Realities, Expectations, Perspectives. *Proektirovanie Budushego. Problemy Tsifrovoy Realnosti: Trudi 1 Mezhdunarodnoy Konferentsii [Designing the Future. Digital Reality Issues: Proc. 6th International Conference (February 8-9, 2018, Moscow)]*. *M.V.Keldysh Institute of Applied Mathematics*. 90-94. Retrieved from: http://keldysh.ru/future/2018/13.pdf doi:10.20948/future-2018-13

Ivanov, V.V.; Malinetskiy, G.G. (2017) Digital Economy: From Theory to Practice. *Innovatsii [Innovations].* 12 (230), 3-12.

Kochkarov, A.A.; Kochkarov, R.A.; Malinetskiy, G.G. (2015) Some aspects of Dynamic Graph Theory. *Zhurnal vychislitelnoy matematiki i matematicheskoy Fisiki [Computing Mathematics and Mathematical Physics Magazine].* 55 (9), 1623-1629.

Kustov, V.N.; Stankevich, T.L. (2019) Blockchain Technology: The Story of Genial Simplicity or Enlightened Mindset. *Zaschita Informatsii. Insaid [Information protection*. *Inside].* 2, 10-18.

Maschenko, P.L.; Pilipenko, M.O. (2017) Blockchain Technology and Its Practical Application. *Nauka, technika, obrazovanie [Science, Technics, Education]*. 32, 61-64.

McGinn, D.; Birch, D.; Akroyd, D.; Molina-Solana, M.; Guo, Y.; Knottenbelt, W.J. (2016) Visualizing Dynamic Bitcoin Transaction Patterns. *Big Data*. 4 (2), 109-119.

Melekhin, I.V. (2019) Blockchain Security: Six Attack Vectors and How to Protect from Them. *Zaschita Informatsii. Insaid [Information protection. Inside]*. 2, 5-9.

Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from: https://bitcoin.org/bitcoin.pdf

Osipovich, S.D. (2019) Qualitative Models and Approaches for Informational Security of Modern Cryptocurrency Financial Systems. *Trudi VI Mezhdunarodnoy Nauchno-Prakticheskoy Conferentsii "Sovremennaya Matematika I Contseptsii Innovatsionnogo Matematicheskogo Obrazovania" [Proc. VI International Academic Workshop "Modern Mathematics and Concepts of Innovative Mathematical Education". Moscow, MFO Publishing*. 498-506.

Petrenko, S.A.; Petrenko, A.S. (2019) About Development of Blockchain Technology in Russia. *Zaschita Informatsii. Insaid [Information protection. Inside]*. 2, 19-25.

Sivakov, O.A. (2019) Blockchain Technologies for Web Applications as a Way to Neutralize IS Risks. *Zaschita Informatsii. Insaid [Information protection. Inside]*. 2, 40-47.

Stugin, M.A. (2019) Protecting Open Information Systems Through Constant Changing. *Zaschita Informatsii. Insaid [Information protection. Inside]*. 2, 34-39.

1. Associate Professor. Department of Data Analysis, Decision Making and Financial Technologies. The Financial University under the Government of the Russian Federation. akochkar@gmail.com

2. Doctoral Student. Department of data analysis, decision making and financial technologies. The Financial University under the Government of the Russian Federation. osipovichsd@gmail.com

3. Associate Professor. Department of Data Analysis, Decision Making and Financial Technologies. The Financial University under the Government of the Russian Federation. rasul_kochkarov@mail.ru

4. https://www.bitmex.com/

https://www.huobi.com/

https://bitforex.com

5. https://www.investing.com/crypto/currencies

Revista ESPACIOS. ISSN 0798 1015
Vol. 41 (Nº 03) Year 2020

[Index]