Часопис из области економије
менаџмента и информатике
Година 2018, волумен 9, број 2, стр. 27-38

Journal of Economics, Management
and Informatics
Year 2018, Volume 9, Number 2, pp. 27-38

Прегледни рад/ Reviewing paper

УДК/UDC: 005.52:330.133.1
339:004.738.5
004.056.55

doi: 10.5937/bizinfo1802027M

COST BENEFIT ANALYSIS OF COMPROMISING LEDGER SYSTEM BASED ON BLOCKCHAIN TECHNOLOGY

ANALIZA TROŠKOVA I KORISTI KOMPROMITIOVANJA SITEMA VREDNOSNOG ZAPISA ZASNOVANOG NA BLOCKCHAIN TEHNOLOGIJI

Edis Mekić[1]
State University of Novi Pazar, Novi Pazar

Safet Purković
State University of Novi Pazar, Novi Pazar

Ahmedin Lekpek
State University of Novi Pazar, Novi Pazar

Abstract: *Modern application of the blockchain technology is the center of attention of technology and economy sectors. Proper usage of blockchain is based on peer to peer (P2P) network to coordinate a worldwide, universal ledger where all transactions on the network are recorded. In order to provide security and veracity of ledger system blockchain systems uses cryptographic hash function. By hashing the block sent by the member of P2P network and checking if it still fits the pattern for the next block, the network can easily prove that the calculating machine did in fact find coded solution of function. Before adding data received on this way majority of the machines on the network must provide consensual confirmation of transaction. this confirmation must be confirmed with at least 51% of machines in the system. This is first and most analyzed vulnerability of this type of ledger systems*

[1] emekic@np.ac.rs

based on blockchain. In this research we analyzed cost benefit analysis for implementation of the proposed attack on three popular block chain systems, and proved that investment in equipment for conducting this type f attack is not beneficial for potential attacker.
Key words: *blockchain, ledger, cost benefit analysis*

Sažetak: *Primena blokchain tehnologije je u centru pažnje kako tehnološkog tako i ekonomskog sektora. Korišćenje blokchain tehnologije zasnovane na P2P sistemima omogućili su stvaranje globalnih univerzalnih sistema vrednosnih zapisa koji sadrže zapise svih transakcija obavljenih u ovim sistemima. Da bi se obezbedila sigurnost i istinitost zapisa blockchain sistemi koriste kriptografske heš funkcije. Rešavanjem ove funkcije svaki blok poslan u P2P sistem se proverava na takav način da se utvrđuje da li je on u skladu sa svim sledećim blokovima. Ako je to slučaj mreža pruža konsenzus koja je mašina zaista rešila ovu funkciju. Ovaj konsensuz se postiže ako transakciju potvrdi najmanje 51% mašina koje su vezane u sistem. Ovo je osnovna i najanaliziranija slabost sistema vrednosnih zapisa zasnovanih na blokchain tehnologiji. U ovom radu je uradjena analiza troškova i koristi za izvodjenje ovakvog napada na tri popularna blokchain sistema, dokazano je da je investicija za izvodjenje ovakvih napada neisplativa za potencijalne napadače.*
Klučne reči: *blockchain, vrednosni zapis, analiza troškova i koristi*

1. INTRODUCTION

Since first introduction of block chain technology on theoretical and practical implementation through bitcoin and alternative digital currency systems, this technology and system based on it attracted lot attention from academia and industry (Desjardins, 2016) .Blockchain was conceived and planned as alternative for traditional payments systems in the wake of economic crisis (Nakamoto, 2008). Simultaneously block chain systems were successfully implemented in the different fields like medicine, economy software engineering etc. (Bylica, et al., 2015; Davidson, De Filippi and Potts, 2016; Ekblaw, et al., 2016; Houy, 2014).

From the economic view traditional systems of following and verifying transaction are heavily centralized systems with defined management and control systems. Important part of this approach is existence of the ledger, or reliable data on completed transaction, which can be verified and without possibility of further manipulation with transaction data (Apte and Petrovsky, 2016).

All block chain technologies are based on highly sophisticated P2P networks and deliver high level of the resistance to compromising data consisting block

chain. This approach overcomes centralized ledger storage since in those systems data on transactions are stored through network. Computers which are involved in the network must conceive consensus that transaction is valid before creation of new entry in to ledger system.

System based on this computational basis create situation were individual transaction computational machines can not endanger system, but also do not provide enough computational power to all network. This forced individuals to form joint pools for increasing of the computational power. With this process weaknesses of the blockchain technology emerged.

First form of attack is providing computational resources to a pool in which a lot of shares have already been submitted and no block has yet been found, individual computational resource will gain less in expectation because the reward will be shared with the miners who have earlier contributed to this pool. Therefore at a certain moment it may be profitable to stop mining in this pool and contribute elsewhere this is so called "Pool Hoping attack" (Desjardins, 2016; Czepluch, Lollike, and Malone, 2015).

Second form is attack where powerful attacker is secretly preparing an alternative version of the block chain. At the same time he is manipulating the automatic difficulty adjustment mechanism in his secret chain in order to increase the probability of eventually that his chain will be recognized as surpassing the public honest chain. If this happens, the attacker reveals his secret chain. This can be used to commit double-spending (Bahack, 2013). This form of attack is known as difficulty raising attack.

In our paper we will describe and analyze feasibility of compromising network using two methods. First is so called The "Mining Cartel Attack" is described in (R. Horning, 2010). It is an attack in which a large fraction of miners such as 51% decide to ignore some or all blocks generated by miners which are not members of the cartel. This allows dishonest miners to achieve higher gains. For the sake of obtaining more realistic results we will propose situation where that type of attack is combining with selfish mining attack which can cut down prices of hardware power needed for compromising block chain based networks (Eyal and Sirer2018).That approach can provide attacker situation where he can overtake block chain with his version of block chain.

Taking over of the blockchain based ledger system is hard achievement. Fixed costs of system for achieving this is rather high (Houy, 2014). In order to properly articulate feasibility we will assume total market cap at the analyzed moment on the network as the value of the assets of ledger system. Then we will calculate investment in the needed hardware power to deliver

and maintain this type of attack, and calculate economic feasibility, and cost benefit analysis of that system.

2. CRYPTOGRAPHIC BLOK CHAIN SYSTEMS

In this work we analyzed three popular blockchain based ledger systems. Every of these system shave different approach and try to resolve different issues which become obvious during first implementation of Bitcoin as first fully implemented blockchain based system.

Blockchain systems are based on the application of cryptographic hash function which are special class of hash function that has certain properties which make it suitable for use in cryptography. Hashing is a mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size (a hash) and is designed to be a one-way function, that is, a function which is infeasible to invert. The only way to recreate the input data from an ideal cryptographic hash function's output is to attempt a brute-force search of possible inputs to see if they produce a match, or use a rainbow table of matched hashes.

As direct result of this any attempt to receive solution for hash function which is needed to create new block into blockchain we need to use calculation power of the computers in P2P network (Naor and Yung 1989). Since data of the total the hash rates of the network are given in any needed time, we will use those data for calculating total value of system which provide feasibility of corrupting block chain system. For the value of ledger assets we will use value of the market capitalization in the moment of collecting data.

First we analyzed Monero system based on the Cryptonote algorithm. This type of algorithm provides fully anonymous transactions satisfying intractability and unlink ability conditions. Unlinkability solution is provided publishing single address and receiving unconditional and unlinkable transaction. In order to create higher level of protection in those systems Cryptonote algorithm involves adjustable parameters for difficulty, size limits and excess size penalty (Van Saberhagen, 2013).

Zcash block chain system is also based on the idea of providing anonymous transactions. Those system is based on implementation of DAP procedure for creating anonymity during transaction, while hashing system is based on the standard SHA-256 Hash function (Sasson, et al., 2014).

Ethereum platform is based on the hash function SHA-3 as a subset of the broader cryptographic primitive family Keccak.Unlike previously implemented block chain systems, which provide only value ledger

(implementation of the virtual currency systems), Eteherum is developed with additional infrastructure for smart contracts, development of blockchain based applications and enterprise software (Bertoni, et al., 2009).

Since all this systems are based on the solving of hash functions, measurement unit for the calculation power of network is hash rate, or number of solved hash functions send to the network. This value is also used is also used in calculations of the blockchain network's overall hash rate. Since each calculating machine or pool of calculating machines only relays a solved block to the network, the overall hash rate of the network is calculated based on the time between blocks. While not an accurate measure of network hash rate at any given instance in time, measurements over longer periods can be considered indicative and similar calculations are used in blockchain difficulty adjustment.

Since all pools have information of the active hash rate of the network in this research we will use those data to calculate average value of singe computer which need to be involved in the process of solving hash functions. After calculating average price we will recalculate needed financial assets and cost benefit analysis, to achieve majority attack on the network and evaluate feasibility toward estimated value of the ledger information based on market cap in the measured time.

3. RESOURCES FOR THE COMPROMISING BLOCKCHAIN NETWORK

Operation of blockchain system is rather simple; we record any changes or transaction within unit of blocks. Blocks are consisted from ID and ID of previous block. Valid block contain solution of hash function problem of previous block, hash function problem solution of new block and address which deliver some kind of prize to solver of this puzzle or transaction fee.

Since theoretically two or more solvers can deliver proper solution to system, those so called double payments are solved by consensus of the computers involved in the solving of hash problem functions. In order to acknowledge blockchain block as valid if 51% of the active machines confirm it as valid, and by the definition it is usually longest block.

Form the beginning of the implementation of those systems it was obvious that entity which have more calculation power will be able to deliver more solution to hash problems and to earn creates more transactions then other network machines. On this way them theoretically can create longest blocks in the system and to refuse to share them during long period of time, and to return to network their own version of blockchain. Since the proof of work in

system is based on consensus that 51% of machines are sufficient to create this type of situation it is called 51% attack.

In order to calculate resources needed for successful implementation of this type of attack during research we first took snapshot of the existing hash rate of network for three proposed networks.

The results are divided in several criteria. The first criteria are to find average hash rate of one machine in the pool. When we found it next step is to found configurations that can reach wanted Hash rate. Average hash rate of the single machine in each pool each pool we calculated using

$$H_{rm} = \frac{\sum_{i=1}^{k} H_{rp_i}}{\frac{H_{rp_i}}{N_{mp}}} \quad (1)$$

Where variate k is total number of pools in network.

4. ANALYSIS OF COMPUTATIONAL POWER AND COSTS FOR EXISTING NETWORKS

The first crypto currency block chain system that we analyzed is Monero. We analyzed four pools and we get data of pool's hash rate, number of calculating machines in that pool and global hash rate of all network. For our analysis we used pools with the most number of calculating machines. In order to provide as much accuracy as possible al monitoring of existing networks were completed in 4:10pm 6.2.2018. For analysis of Monero network we used following pools: Pool number 1: https://web.xmrpool.eu/; Pool number 2: http://minexmr.com/; Pool number 3: https://monero.crypto-pool.fr/; Pool number 4: https://monerohash.com/. Total network hash rate of all network was 819.68 10^6 H/sec, and calculated hash rate using (1), or computational calculated power for each machine in network is given in table 1.

Table 1. Monero network computational power per machine

Rows	Pool Hash rate (H/sec)	Pool calculating machines	Hash rate per machine(H/sec)
1	2,860 10^3	1.980 10^3	1,444.00
2	46,770 10^3	27.195 10^3	1,719.80
3	16,440 10^3	1.849 10^3	8,891.29
4	7,370 10^3	2.757 10^3	2,673.19

Average hash rate per machine is: 3682.07 H/sec.

At the same time we completed overlook of the Zcash network using following pools:

- Pool number 1: https://zec.nanopool.org/;
- Pool number 2: https://zcash.flypool.org/;
- Pool number 3:https://zec.suprnova.cc/index.php?page=gettingstarted.

Total network hash rate at spotted moment was 341,856.70 KSol/s. Computational power is provided in table 2

Table 2. Zcash network computational power per machine

Rows	Pool Hash rate (Sol/sec)	Pool calculating machines	Hash rate per machine(Sol/sec)
1	53,778	35.057	1,534.01
2	244,500	150.114	1,624.76
3	6,411.72	4.727	1,356.40

Average hash rate per machine is:: 1505.06 Sol/sec.

Third network computational power was calculated using data acquired from three distinguished pools:

- Pool number 1: https://eth.2miners.com/en;
- Pool number 2: https://eth.suprnova.cc/index.php?page=statistics&action=pool
- Pool number 3: https://eth.nanopool.org/?_ga=2.135956788.446524210.1518515681-537509725.1517934497.

At the moment of calculating value of network hash rate was 195.62 TH/s. Hash rate per machine engaged in computation on the mentioned pools is given in table 3.

Table 3. Zcash network computational power per machine

Rows	Pool Hash rate (H/sec)	Pool calculating machines	Hash rate per machine(MH/sec)
1	$221{,}640*10^6$	776	285.66
2	$36{,}533{,}000*10^6$	93,264	391.71
3	$92{,}536*10^6$	665	139.15

Calculated average hash rate per machine is272.17 MH/sec.

5. VALUE OF THE HARDWARE CONFIGURATIONS PROVIDING AVERAGE HASH RATE PER MACHINE

In order to calculate value and economic feasibility of the attack on the blockchain networks, we decided to establish price of the configurations which can achieve requested hash rates.
Average price per machine we count as sum of all configurations as

$$APPM = \frac{\sum_{i=1}^{n} P_i}{N_m} \quad (2)$$

APPM - average price per machine,
N_m- number of configurations,
P_i – Average price of single configuration.

GPU and CPU benchmarks for Monero are available on http://monerobenchmarks.info/ and presented on table 4 , for Zcah on http://www.zcashbenchmarks.info/ presented on table 4 and for Ethereum on https://www.techspot.com/article/1438-ethereum-mining-gpu-benchmark/ presented on table 6.

Table 4. Monero network computational price range of machines matching average H_{rm}

Rows	GPU	Motherboard	Hash rate (H/sec)	Price ($)
1	2 X VEGA 56	MSI - Z370 GAMING PLUS ATX LGA1151	3,700	2115
2	5X SAPPHIRE RX 580 NITRO+ AND R3 1300X CPU 4 CORES	MSI - Z370 GAMING PLUS ATX LGA1151	3,700	2715
3	6X XFX R9 380	MSI - Z370 GAMING PLUS ATX LGA1151	3,743	2335

Table 5. Zcash network computational price range of machines matching average H_{rm}

Rows	GPU	Motherboard	Hash rate (H/sec)	Price ($)
1	2X ASUS 1080 TI STRIX OC	MSI Z87 MPOWER MAX	1,550	3000

2	6X GIGABYTE GTX 1060 6GB (MICRON)	MSI Z270 GAMING PRO CARBON	1,980	3265
3	4X ZOTAC GTX 1070 AMP! CORE EDITION	ASUS ROG Maximus VIII FORMULA	2,006	4210

Table 6. Ethereum network computational power per machine

Rows	GPU	Motherboard	Hash rate (MH/sec)	Price ($)
1	7x GeForce GTX 1080 Ti	MSI Z87 MPOWER MAX	281.7	11100
2	7x Radeon RX Vega 56	MSI Z87 MPOWER MAX	291.68	8300

Monero: APPM= 3,025.33$

Zcahsh APPM= 4,086.67$

Ethereum APPM= 10,295$

6. COSTS BENEFIT AND FEASIBILITY OF CORRUPTING BLOCKCHAIN BASED SYSTEM

In order to provide exact calculations for price of the computational power first we need to determine number of the machines which need to exist in our compromising pool in order to provide successful attack. Also we deliver Coinmarket cap as the total value of the ledger components (we do not calculate coin market or similar value, we presume that with this level of blockchain system value of the data in network is equal to Coinmarket cap)

First we calculate umber of Miners in network counts as network Hash rate divided by average Hash rate per machine:

$$N_m = \frac{H_{rp_i}}{N_{mp}} \quad (3)$$

Then we calculate price based on average price of single machine P, and deliver cost benefit value as ratio of market cap and investment in machines.

Table 7. Feasibility and cost benefit ratio of compromising networks

	N_m	P	Cap	Cost benefit ratio
Monero	222614	343,474,790.89	2,414,280,000	1:7,02
Zcash	718741	479,399,852.80	1,110,095,870	1:2,34
Ethereum	227138	3,773,704,315,00	6,098,854,819	1:1,16

In our example we used Cost benefit analysis based on the simplified model were we calculated investment cost based on the calculation of the raw calculating machines needed for compromising blockchain systems. We did not included analysis of the operational and additional maintenance costs which would additionally lower cost benefit ratio. If we presume that those costs can achieve up to 20% of the investment, cost benefit analysis show that for while it is economically feasible compromising first two networks third become non benefit (CBR 0,982). Since all networks are in this time expand number of the engaged computers in the P2P network it is safe to assume that other networks would be in negative CBR soon. Since financial institutions are aware that existing system of the management control, revision and accounting system is inefficient and expensive (Davidson, De Filippi and Potts, 2016). Existing system is not adequate for implementation in modern technological and global market, on other side blockchain as decentralized system provide flexibility, efficiency stability and high level f the security toward potential security breaches as we show in our analysis.

7. CONCLUSION

In this work we combined two approaches to solve issue of compromising blockchain based ledger system. First is calculating sheer computational power need for the compromising network. After calculation of the number and hash rate of the machines needed to successfully deliver this type of attack we used economical tools to evaluate value of the investment of network. Those data were used to calculate cost benefit ratio toward total value of the ledger system (market capitalization). We showed that after normalization with running costs that type of attack are expensive and hard for implementation.

During research it became obvious that blockchain is important cross issue between economics, mathematics and informational technologies. All critical part of the systems is connected by the state of the art protection systems aka cryptographic, distributed network and economic feasibility. Results opened important questions for further research like connection of the number of data and implementing price of system, level of transaction fees, establishing self regulated blockchain system as alternative to existing financial institutions,

development of high calculating systems and sophisticated coding and decoding techniques for hash functions.

REFERENCES

1. Apte, S. and Petrovsky, N., 2016. Will blockchain technology revolutionize excipient supply chain management?. *Journal of Excipients and Food Chemicals*, *7*(3), p.910.
2. Bertoni, G., Daemen, J., Peeters, M. and Van Assche, G., 2009. Keccak sponge function family main document. *Submission to NIST (Round 2)*, *3*(30).
3. Bylica, P., Glen, L., Janiuk, P., Skrzypcaz, A. and Zawlocki, A., 2015. *A Probabilistic Nanopayment Scheme for Golem*.
4. Bahack, L., 2013. Theoretical Bitcoin Attacks with less than Half of the Computational Power (draft). *arXiv preprint arXiv:1312.7013*.
5. Czepluch, J.S., Lollike, N.Z. and Malone, S.O., 2015. The use of block chain technology in different application domains. Copenhagen: The IT University of Copenhagen.
6. Davidson, S., De Filippi, P. and Potts, J., 2016. *Economics of blockchain*.
7. Desjardins, J., 2016. It's official: Bitcoin was the top performing currency of 2015. Available at: <http://money.visualcapitalist.com/its-official-bitcoin-was-the-top-performing-currency-of-2015/> [Accessed 17 September 2018].
8. Ekblaw, A., Azaria, A., Halamka, J.D. and Lippman, A., 2016, August. A Case Study for Blockchain in Healthcare:"MedRec" prototype for electronic health records and medical research data. In *Proceedings of IEEE open & big data conference* (Vol. 13, p. 13).
9. Eyal, I. and Sirer, E.G., 2018. Majority is not enough: Bitcoin mining is vulnerable. *Communications of the ACM*, 61(7), pp.95-102.
10. Houy, N., 2014. *It Will Cost You Nothing to'Kill'a Proof-of-Stake Crypto-Currency*.
11. Nakamoto, S., 2008. Bitcoin: *A peer-to-peer electronic cash system.*
12. Naor, M. and Yung, M., 1989, February. Universal one-way hash functions and their cryptographic applications. In *Proceedings of the twenty-first annual ACM symposium on Theory of computing* (pp. 33-43). ACM.
13. Rosenfeld, M., 2011. Analysis of bitcoin pooled mining reward systems. *arXiv preprint arXiv:1112.4980.*
14. Rosenfeld, M., 2013. *Mining pools reward methods*. In Presentation at Bitcoin 2013 Conference.
15. RHorning, 2010. Mining cartel attack. *Bitcoin Forum*, [blog] 22 December, Available at: <

https://bitcointalk.org/index.php?topic=2227> [Accessed 15 September 2018].
16. Sasson, E.B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E. and Virza, M., 2014, May. Zerocash: Decentralized anonymous payments from bitcoin. In *2014 IEEE Symposium on Security and Privacy (SP)* (pp. 459-474). IEEE.
17. Van Saberhagen, N., 2013. CryptoNote v 2.0.
18. Zhang, Y. and Wen, J., 2017. The IoT electric business model: Using blockchain technology for the internet of things. *Peer-to-Peer Networking and Applications*, 10(4), pp.983-994.

Received: 5 October, 2018
Accepted: 11 November, 2018