Empirical Analysis of Silent Mining Operation in the Monero System

Safet PURKOVIC[1]*, Edis MEKIC[1], Kristijan KUK[2], Ladin GOSTIMIROVIC[3]

[1] State University of Novi Pazar, Vuka Karadzica 9, Novi Pazar, 36310, Serbia
spurkovic@np.ac.rs (**Corresponding author*), emekic@np.ac.rs

[2] The Academy of Criminalistic and Police Studies, 196 Cara Dsana, Belgrade, 11080, Serbia
kristijan.kuk@kpu.edu.rs

[3] College of Business and Technical Education in Doboj, Ozrenskih srpskih brigada 5A, Doboj, 74000, Bosnia and Herzegovina
direktor@vpts-doboj.info

Abstract: This paper analyses three important issues regarding Blockchain systems. The first one is related to the existence, success and mitigation of silent mining activity achieved through the development of Application-specific Integrated Circuits (ASICs). The second one lies in the mathematical modelling of Blockchain systems affected by ASIC mining machines and in the mathematical modelling of Blockchain with suppressed ASICs. Finally, this paper presents the economic parameters related to the rate of Return on Investment (ROI) and the possibility of calculating them based on the obtained results. Three different Blockchain systems were analysed, two of which allow the usage of ASIC machines, while one of them by definition does not support this type of mining activity. The analysis showed that the systems which involve ASIC machines can be described by means of linear regression models, while suppressing ASICs mining would provide a different statistical model. Successful mitigation activities can provide reliable data for the calculation of the economic parameters related to the rate of Return on Investment (ROI) based on silent mining.

Keywords: Silent mining, ASIC machines, Monero system, Blockchain.

1. Introduction

Creating a secure ledger system, without third party control over data stored in it is at the focus of economic, mathematical and computer technologies research. The development of Blockchain technology provided one possible answer to this problem and bound all those scientific disciplines.

Blockchain technology provided a decentralized transaction system for keeping ledger inputs. New inputs in the Blockchain ledger are possible only after confirmation from the majority of network members. Public ledger is accessible to all computers of the network or nodes. At the same time nodes are anonymous and this system provides a higher level of security in process of confirmation of transactions in comparison with traditional ledger systems (Zyskind, Nathan & Pentland, 2015).

Transactions in Blockchain system are grouped in blocks. Security of block creation and validation process are based on cryptographic hash function. Hash functions represent a special class of mathematical functions with certain properties which make them suitable for use in cryptography. Hashing is a mathematical algorithm that maps data of arbitrary size to an array of fixed-size bits (a hash). This algorithm is a one-way function, which is a function 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 (Rogaway & Shrimpton, 2004).

A new block references an older block by solution of hash function and this solution is header of older block. Speed of the calculation of the proper solution is an important issue in Blockchain implementation. If one can provide more possible solutions of hash functions in time period after last exact solution is calculated, then one has better chances of providing the exact solution.

Blockchain systems also require consensus for validation of transactions, as additional level of security. Only after majority validates transaction, change in data and creation of new block within Blockchain systems is approved by this consensus algorithm. Consensus is provided by the majority of the machines interconnected in P2P networks. These machines solve hash functions and submit solutions to network until the successful solution is calculated. The creation of new blocks into block chain, requires considerable calculation power of the computers interconnected in (P2P) network (Mekić, Purković & Lekpek, 2018).

https://doi.org/10.24846/v30i4y202109

Number of solution submitted to network in designated period of time, which is usually one second, is Hash Rate (HR) of system. Calculating power in network can be provided by Computer Processors (CPU), Graphic Processor Units (GPU) or Application-specific Integrated Circuits (ASICs). ASIC machines can provide substantial hashing power since they are more effective in solving hash functions than CPU- or GPU-based calculating machines.

Successful solution of Hash function is rewarded with a certain amount of cryptocurrency. This calculation and rewarding process is known as mining. Attacks for compromising Blockchain are based on providing most of the hashing power to system in order to change, compromise data or getting the upper hand in mining over other mining entities (Vasek, Thornton & Moore, 2014). Most of hashing power can be acquired by purchase of the calculating machine (Central processing unit (CPU) or Graphic processor unit (GPU) based) or by development of machines based on Application-specific Integrated Circuits (ASICs). ASIC machines represent hardware specialized for solving exact hashing functions. Any change in the core hashing routine can make those machines obsolete (Kurzweil et al., 1990). Important issues arise, for example, what if ASICs manufacturers develop machines for Blockchain systems which by definition do not encourage this type of mining but relay on GPU and CPU mining in order to provide maximal decentralization? And if manufacturer develop those machines can they use this ASIC machine to compromise system without knowledge of core team in silent mining operation? Finally, if this happens can one use properties of Blockchain system to detect this type of operation?

HR of the network can provide data on calculating power of system, but it is impossible to recognize the type of calculating machine which provides HR. This is the reason why the majority of research lacks empirical evaluation of Blockchain effectiveness on privacy and security issues. Security and privacy breaches are usually analyzed by tracking online forums and posts on those topics (Vasek & Moore, 2015).

Empirical analysis of silent mining activities is analyzed on the Monero CryptoNight-based Blockchain system. CryptoNight Blockchain network does not support ASICs mining. The system relies on CPU and GPU mining and in this way its aim is to avoid concentration of sustainable calculating power out of reach of small miners. This approach provides a wide-area distributed system which is resistant to centralization (van Saberhagen, 2013).

HR change and trend analysis in Blockchain system based on CryptoNight algorithm can be employed in order to empirically prove the existence of the ASIC machines and their misuse. In this paper one statistically calculates accuracy of the linear regression model applied during time period when ASIC machines were used with time periods when mitigation effects were applied by core development team. It is shown that systems which support free application of ASIC machines are following symmetrical linear regression functions. When ASIC machines are removed different functional patterns occur. Symmetrical fitting provides empirical proofs for misusage and successful attacks on the system.

The analysis will also provide empirical proof of efficiency of the measures taken by the algorithm development team in order to mitigate effects of silent mining ASIC machines in Blockchain system. The trends of HR change are compared with two other Blockchain systems which allow free usage of ASIC machine to prove empirical findings.

Results of the research are used in order to provide cost benefit analysis of the action and effects of measures applied by the core team for avoiding and mitigating silent mining activity.

The analysis of the research in the field of Blockchain technologies showed that this research field has attracted a great number of young researchers. Based on the literature reviews several main fields of research were established: Blockchain framework, Blockchain algorithm, Blockchain mining, Blockchain modelling, Blockchain in cloud computing environment, distributed computing and Blockchain, Blockchain methodology, P2P structures, data privacy and security (Gorkhali et al., 2020).

After the analysis of the existing literature, authors to the best of their knowledge, find a scarce amount of statistical analysis of the Blockchain processes. Since Blockchain can be applied in different sciences this work will provide an additional point of view on this topic.

The remainder of this paper is structured as follows. Section 2 presents main research hypotheses on data collected. Section 3 sets forth the methodology used for hypotheses testing. Section 4 discusses the results obtained for the implemented methodology. Finally, the conclusions are derived in Section 5.

2. Research Hypotheses and Data

This study is based on the following research hypotheses.

H1. Influence of the ASIC machines on the overall HR of system can be calculated and empirically analyzed by symmetrical linear regression models;

H2. Symmetrical regression models and trends for HR change for the systems in which ASIC machine mining is allowed and are statistically different from equivalent models in the systems where ASIC machine mining is forbidden;

H3. Empirical analysis of those trends can provide information about silent mining activity and efficiency of mitigation effort in Blockchain systems;

H4. The result of the analysis can be used to calculate ROI parameter of implementation of this activity.

The representative network for analysis will be CryptoNight hashing algorithm based Monero Blockchain systems. CryptoNight-based Blockchain systems should be mineable only by GPU- or CPU- based machines. Implementation of this approach protects small mining entities, and rules big centralized systems out of the game. Development of other Blockchain systems showed that ASIC machines with high calculating power can be used for centralizing calculating power of mining entities. The long-term effect would be centralization of system. HR of additional networks which allow free usage of ASIC machines will be analyzed in order to provide additional inputs and comparison with the process analyzed in Monero network.

Those problems were carefully investigated during preparation of Monero Whitepaper (van Saberhagen, 2013). First part of the document covered problems of traceability of Bitcoin transactions. In order to establish untraceability Monero relied on cryptographic primitive traceable ring signature established by Fujisaki & Suzuki (2007).

Other issues are related to egalitarian approach (equal treatment of all miners in system) and how to deny miners on ASIC machines or GPU to create majority of calculating power, by diminishing calculating power of CPU based miners. This is solved by proposing the innovative Proof of Work (PoW) approach. The proposed PoW is memory-bound to 2Mb for scripting new blocks. This is due to several reasons. This block fits into L3 cache memory of modern CPUs, and this amount of memory is unacceptable and expensive for implementation in ASIC machines. GPU processors while capable of completing a huge amount of calculations are limited in memory speed which is slower than that of L3 cache.

A HR change over time is a good indicator for estimating the number of machines involved in calculation endeavor. The main problem is that the different sources of calculation power are indistinguishable in overall HR. HR is subject to highly fluctuating changes when Blockchain systems go through Hard Fork (HF) or when new versions Blockchain algorithm are introduced.

Empirical analysis was carried out by taking highest amount of Blockchain network HR. HR_{max} before HF is taken as maximum value. This value was used for calculating percentage drop of HR during recovery time period. Values of the HR are given in (Anon, 2020a).

Starting point of analysis was the release of Monero v0.10, the so-called Wolfram Warptangent revision, this was a mandatory update based on previously planned HF activities. The reason for this HF implementation was unexpectedly high adoption rate of RingCT transactions. This created an environment where modification of the dynamic block size limiting algorithm was necessary.

The second point of analysis was the release of Helium Hydra v0.11.0.0 of the Monero software. This was a mandatory update which increased the minimum ring signature size to 5 across the network (this mean that five inputs will be pulled from user wallet, which will then be added to the ring signature transaction. Four inputs are past transaction outputs that are pulled from the Monero Blockchain. These four inputs are decoys, and when fused with the input from user wallet, forms a group of five possible signers), banned duplicate ring members in a ring signature and enforced use of RingCT for all transaction outputs. This release of the software brought major improvements to Monero network system.

After this release Bitmain Technologies Ltd., or Bitmain world's largest developers of Application-specific integrated circuit (ASIC) chips for Bitcoin mining announced that they developed ASIC machines for successful mining of all CryptoNight-based Blockchain systems (Bitmain Technologies Ltd., 2018). Introducing of the ASIC machine would have immediate and obvious effect on overall HR of the system. ASIC machines would ignite the trend of sudden HR change and increase.

Monero community decided that next planned HF of the system will enable the implementation of the new PoW algorithm. Theoretically this would render ASIC machines unusable. On the day of Bitmain announcement, core developer Riccardo "Fluffypony" Spagni declared "Between now and then I will do everything in my power to help the community prevent the proliferation of centralization-inducing ASICs on the Monero network" (Williams-Grut, 2018).

The Monero core team prepared the release of Lithium Luna v0.12.0.0, which represents the third point of analysis. This major release increased the minimum ring signature size, sorted inputs to disable leak wallet choice by inference, and slightly changed the Proof-of-Work algorithm to prevent mining activities by ASIC machines.

This release of the software brought about a number of major improvements to Monero, as well as a large set of fixed bugs. This release is also part of the mitigating effort related to suspected silent mining activity with ASIC machines. During this period the analysis carried out will show effects of mitigation activities applied by core team.

The fourth point of analysis was the release of Beryllium Bullet. This is the v0.13.0 release of the Monero software. This major release enabled Bulletproofs for reduced transaction sizes, set the ring size globally to 11 for uniformity of transactions, updated the PoW algorithm to CNv2, and finally set the max transaction size at half of the penalty-free block size.

The fifth point of analysis was the release of Boron Butterfly v0.14.0 of the CryptoNight routine. This major release added a new PoW based on CryptoNight R algorithm, added a new block weight algorithm, and introduced a slightly more efficient RingCT format. This is an intermediary, stable release specifically for the network update, and does not represent the bulk of the effort on Monero. That effort was completed in the release 0.14.1, which followed during March 2019. after the network update. The results of this update up to latest date were analyzed to reveal possible new silent mining operation between v0.13.0 and v0.14.0 releases.

Symmetrical regression models were used in order to analyse HR change of Ethereum network after HFs. This Blockchain system supported ASIC mining. HR was analysed for a six-month period after Byzantium HF on 16/10/2017. Another set of values for Ethereum was analysed after Constantinople HF on 28/10/2019. Subsequent HFs were not analysed since the implementation of the new algorithm rendered ASICs mining unavailable on this platform. Detailed values of HR are taken from (Anon, 2020b).

Values of HR are given in Figure 1 for Ethereum network (expressed in Tera Hashes per second) and in Figure 2 for Monero network (expressed in Mega Hashes per second).

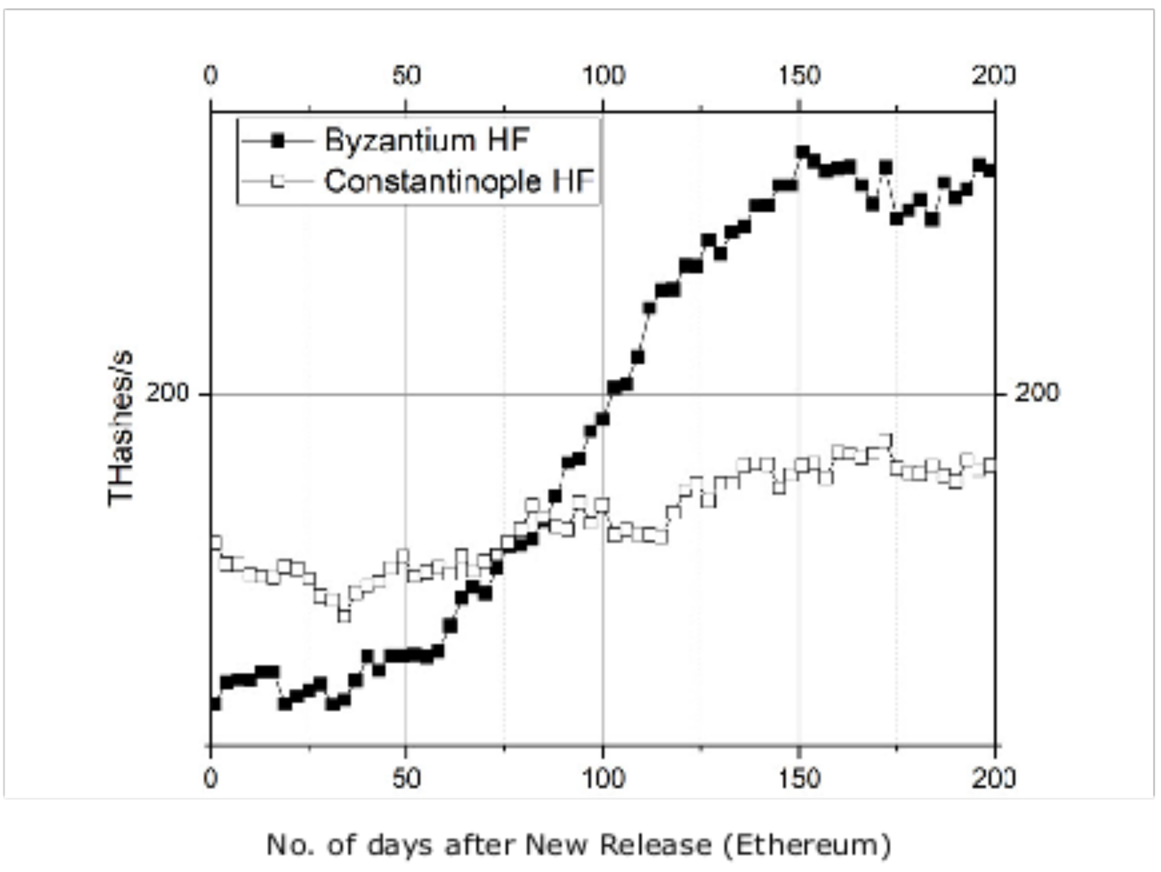

Figure 1. HR values for Ethereum network

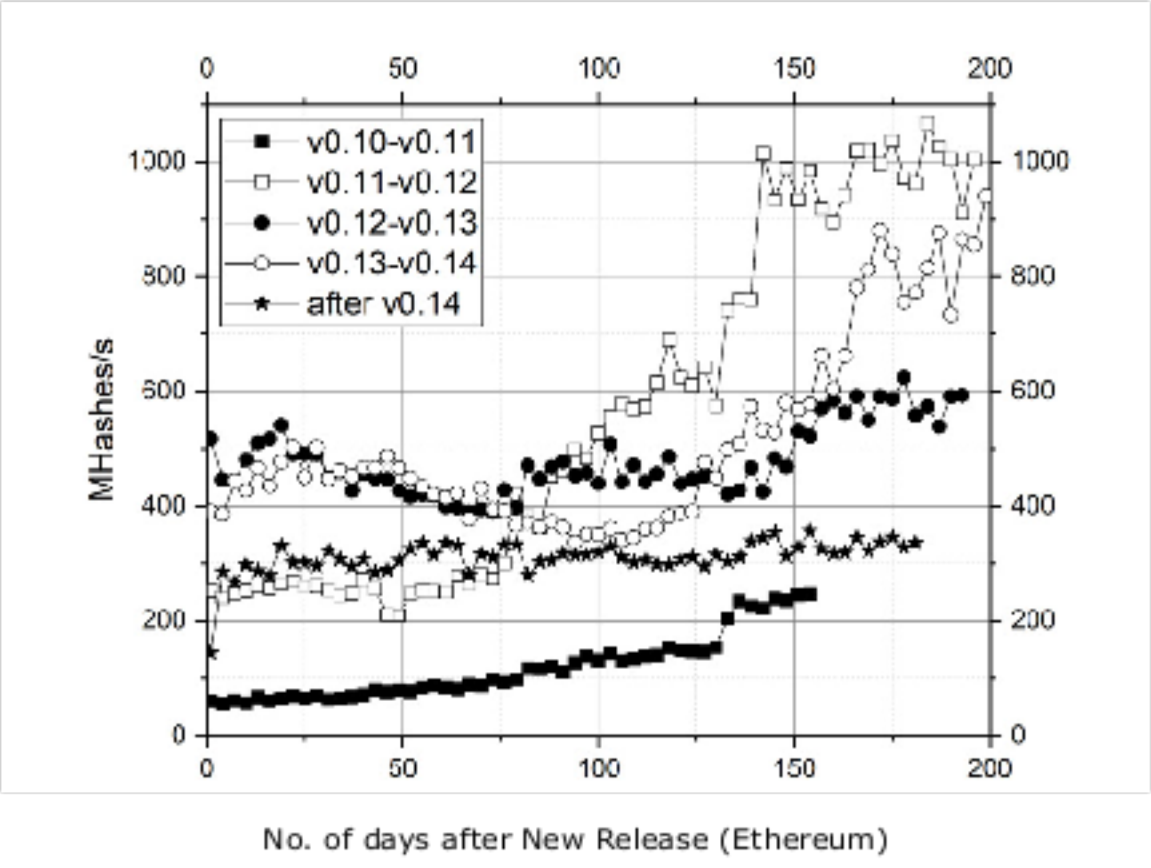

Figure 2. HR values for Monero network

3. Methodology

Empirical analysis was based on Symmetrical Linear Regression model (Bevington & Robinson, 1969) explained by implemented on the data set ($d_{i,hi}$), i=1,2,..n. The value of d_i is *i - 1* number of days after HF when average HR for that date is measured and $h_i = \frac{H_{avri}}{H_{max}}$ is ratio of the average HR on the i-1 days after HF to the maximal value of HR before HF.

Linear regression model for proper fitting of data is given as follows (Edwards, 1976).

$$h_i = \beta_0 + \beta_1 d_i + \varepsilon_i \tag{1}$$

For given data set d_i is an independent variable and h_i is a dependent variable, ε_i is a random error term with mean $E\{\varepsilon_i\} = 0$ and β_0 and β_1 are parameters defined in the following way:

$$\hat{\beta}_1 = \frac{SDH}{SDD} \tag{2}$$

$$\hat{\beta}_0 = \overline{h} - \beta_1 \overline{d} \tag{3}$$

In order to calculate proposed datasets, the missing parameters $\bar{d}$, $\bar{h}$, *SDH* and SDD will be defined in the following way:

$$\overline{d} = \frac{1}{n}\sum_{i=1}^{n} d_i, \overline{h} = \frac{1}{n}\sum_{i=1}^{n} h_i \tag{4}$$

$$SDH = \sum_{i=1}^{n} d_i h_i \tag{5}$$

$$SDD = \sum_{i=1}^{n} (d_i - \overline{d})(h_i - \overline{h}) \tag{6}$$

In order to check viability of fitting model several additional parameters were calculated and analyzed.

The first parameter is residual sum of squares. This parameter is the sum of the square of the vertical deviations from each data point to the fitting regression line. Perfect fit is achieved if the value of RSS is equal to zero. The smaller the residual sum of squares, the better the proposed model fits collected data. This value is calculated using the following formula, where ω_i is the root of variance.

$$RSS = \sum_{i=1}^{n} \omega_i [h_i - (\beta_0 + \beta_1 d_i)]^2 \tag{7}$$

The second parameter is Pearson's correlation coefficient, Pearson's r. Pearson's r denotes the strength of linear relationship between paired data. The value of Pearson's r can be between -1 and 1. Positive value of Pearson's r indicates that there is positive linear correlation between predictor variable and response variable. The value of zero indicates that there is no linear correlation between paired data. If its value is negative there is negative linear correlation. There is a stronger linear correlation if this value tends towards -1 or 1 (Vasek & Moore, 2015; Vasek, Thornton & Moore, 2014).

The final parameter is R-square, also known as the coefficient of determination (COD). It is a percentage of the response variable variation that can be explained by the fitting regression line.

Finally, security and reliability of Blockchain networks is in close relationship with hashing power introduced in the system. Further on, the cost-benefit analysis of possible silent mining attacks in the Blockchain system is presented.

In this case, a simplified cost benefit analysis was used, whereby the number of required ASIC machines was taken as a basis in order to achieve the heights of the observed period.

The number of active machines was obtained as the ratio between the difference between the HRs in two periods before the HF and HR of ASIC machine provided in technical specification of the same.

$$N_m = \left(H_{M\max} - \sum_{i=1}^{n} \frac{H_i}{n} \right) / H_{ASIC} \tag{8}$$

The calculated power of ASIC machine Antminer X3 was $H_{ASIC} = 220\ KH/s$, while power consumption was 465W.

By multiplying the number of required ASIC machines and their average price on the market, the purchase cost for the machine was obtained.

Using Monero mining profitability calculator one obtained the amount of the realized profit at the monthly level and the corresponding electricity costs (where the price of 1KW / h was taken as 0,21 $), while neglecting other costs. The benefits also included the profit that was to be generated by the subsequent sale of the ASIC machines mentioned above.

4. Results and Discussion

The analysis of the values of the Residual Sum of Squares presented in Table 4 shows that one-way ANOVA symmetrical linear fitting can be applied in order to describe the system functioning.

The results of this analysis indicate the possibility that they be the results of certain random processes which are not in line with symmetrical fit namely, under the 0.05 level. Those random processes are introduced by additional calculation power from superior calculating algorithms. All analyzed cases can be modeled with symmetrical linear fitting models.

After establishing these it is necessary to check if the proposed fitting models are appropriate in all analyzed cases. It is necessary to establish if there is a statistical difference between fitting models when there are ASIC machines in the system, and when the ASIC machines are disabled.

First, data is analyzed for all instances where ASIC mining is allowed or suspected. The trend between v.010 and v.011 CryptoNight releases shows a strong correlation between predicted and response value (Pearson's r value of 0.92667) and this model reaches a variation of over 85% (COD value 0.85873). Fitting is illustrated in Figure 3.

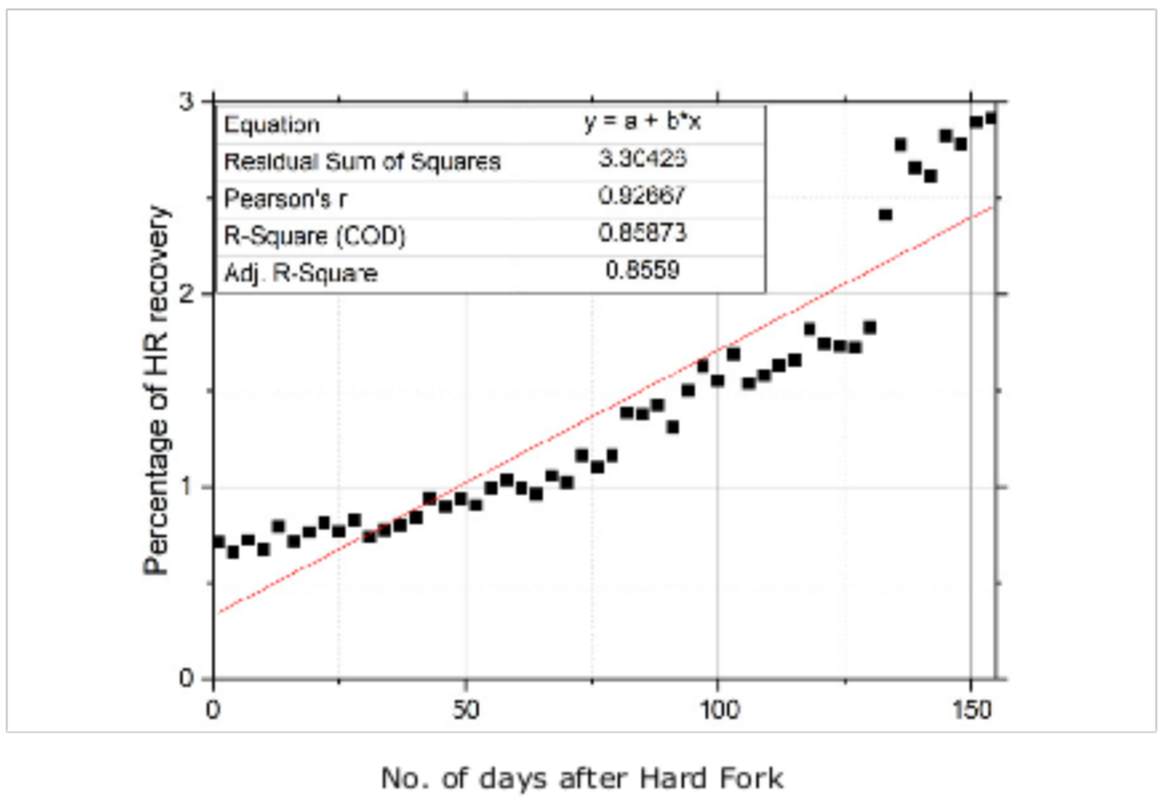

Figure 3. HR trend between v.010 and v.011 CryptoNight releases

The trend between v.011 and v.012 CryptoNight releases shows a strong correlation between predicted and response value (Pearson's r value of 0.94576) and this model reaches a variation of over 89% (COD value 0.89447). Fitting is illustrated in Figure 4.

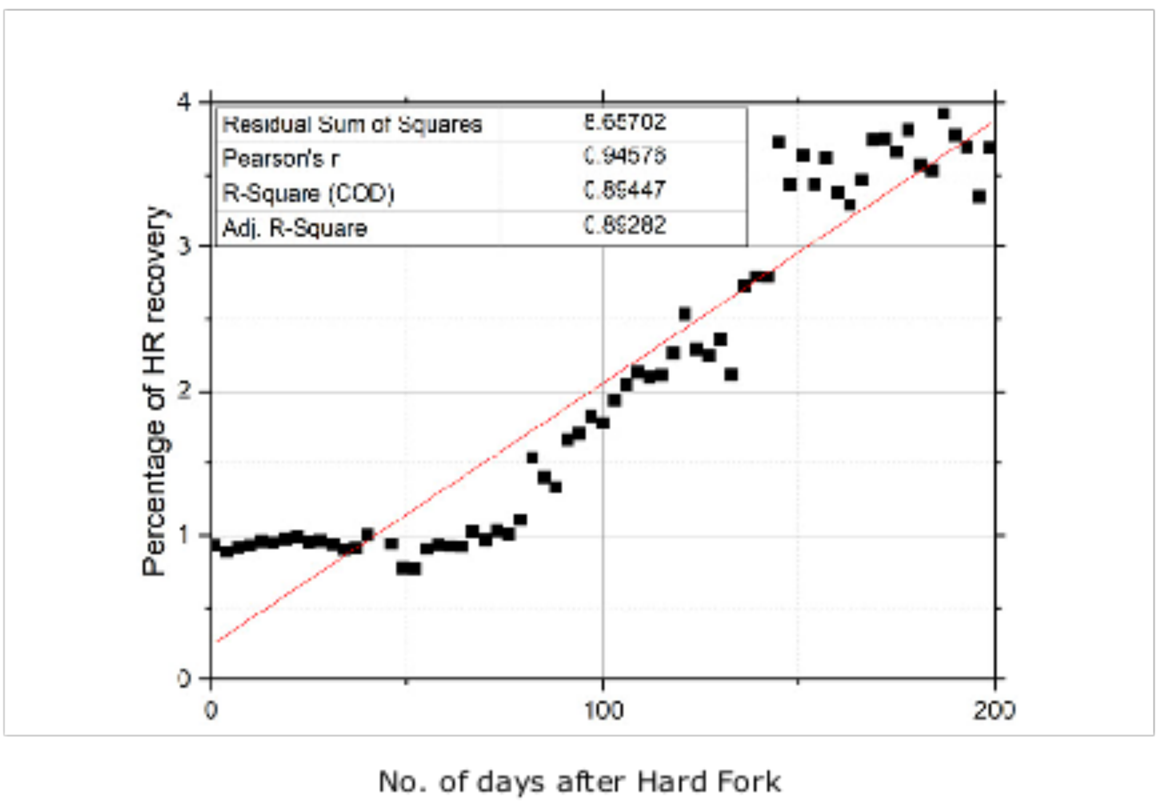

Figure 4. HR trend between v.011 and v.012 CryptoNight releases

Similar trends can be observed in the two proposed Ethereum-based systems. Fitting after Byzantium HF shows a strong correlation between predicted and response value (Pearson's r value of 0.95962) and this model reaches a variation of over 92% (COD value 0.92087). Fitting is illustrated in Figure 8.

Fitting after Constantinople HF shows a strong correlation between predicted and response value (Pearson's r value of 0.91571) and this model reaches a variation of over 83% (COD value 0.83853). Fitting is depicted in Figure 9.

The same analysis was carried out for the instances where ASIC mining was disabled.

Fitting of the trend between v.012 and v.013 CryptoNight releases shows lower level of correlation between predicted and response value (Pearson's r value of 0.53631). The fitting for this model reaches a variation slightly over 28% (COD value 0.28763). Fitting is illustrated in Figure 5. A small value of variation was expected since this change not only excluded ASIC machines, but also required reinstallation of the complete set of mining software on all machines in the system. This means that in this case only slightly over 28% of calculating machines were ready for update. By contrast, in the former examples with ASIC machines they provided most of the calculating power, and they did not need adaptation or update to continue providing HR. So, in this case there is an inappreciable transition in HR between different HFs.

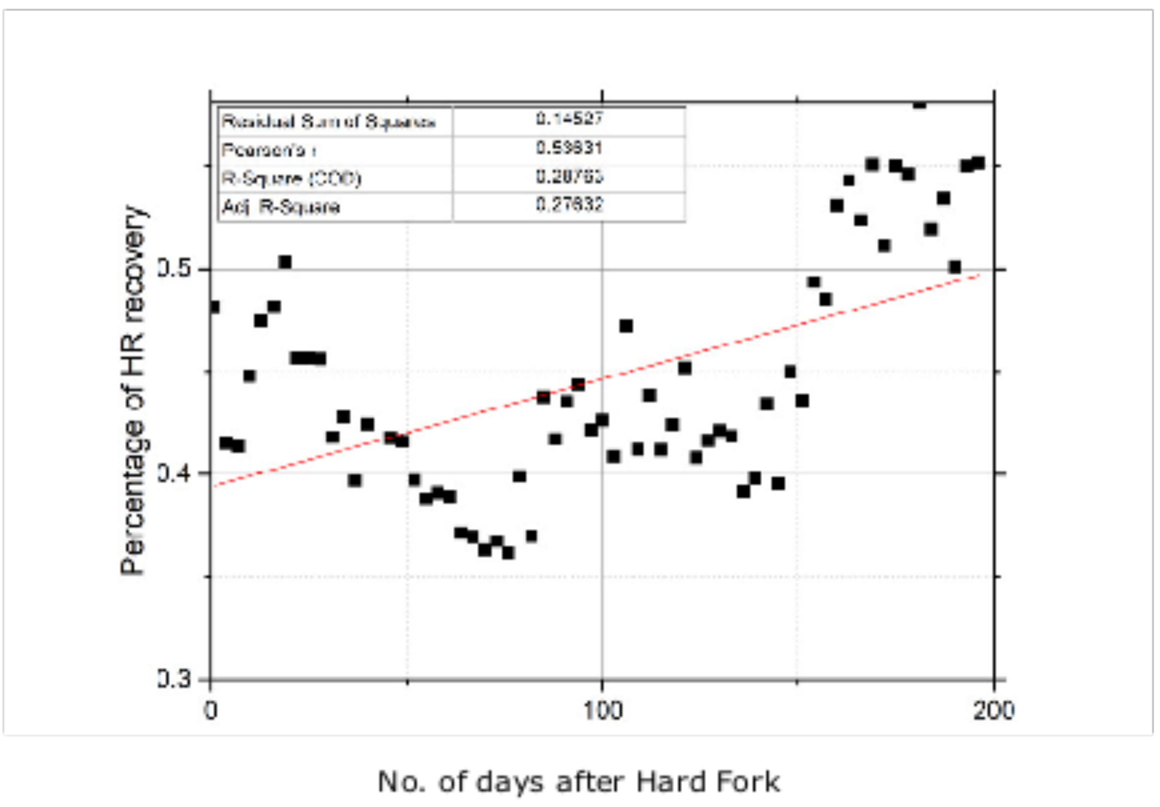

Figure 5. HR trend between v.012 and v.013 CryptoNight releases

A similar trend continues if one analyzes HR between v.013 and v.014 CryptoNight releases. There is a lower correlation between predicted and response value (Pearson's r value of 0.68447) and this model only reaches a variation slightly over 46% (COD value 0.4685) Fitting is illustrated in Figure 6.

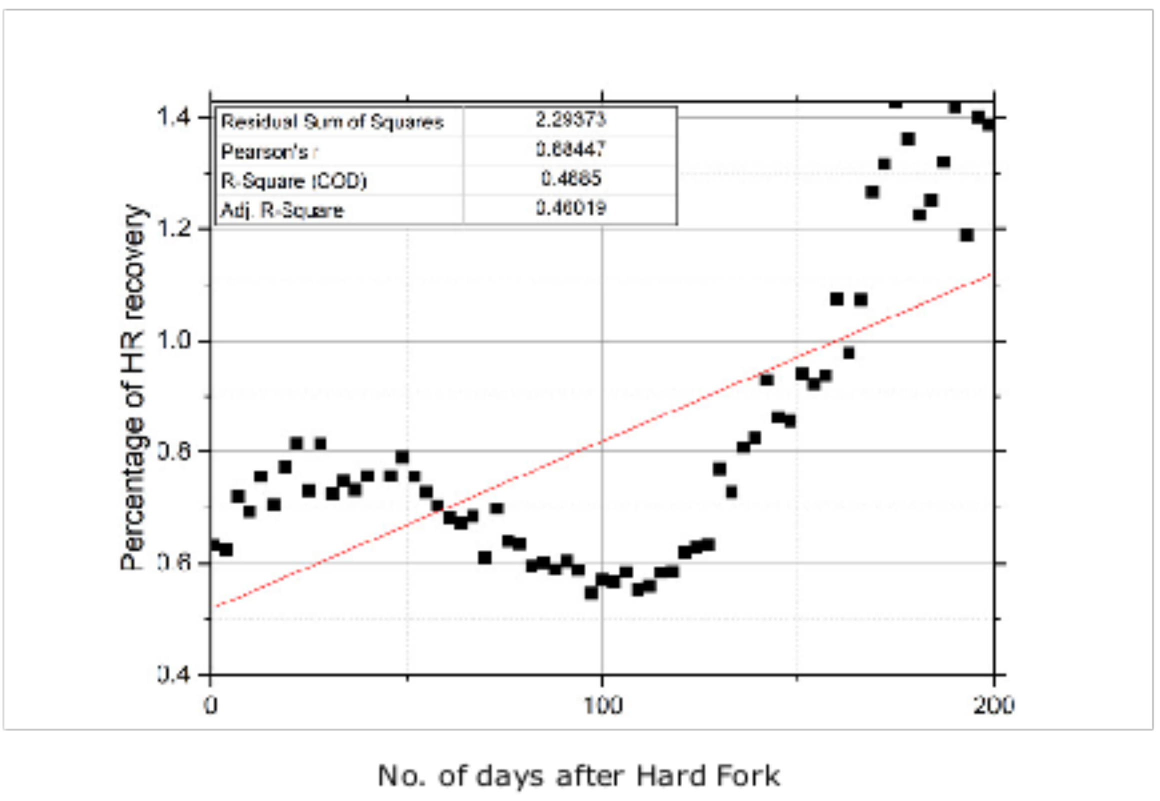

Figure 6. HR trend between v.013 and v.014 CryptoNight releases

Finally, the analysis of HR trend continued after v.014 CryptoNight release and it shows a similar correlation trend between predicted and response value (Pearson's r value of 0.53291) and this model only reaches a variation slightly over 28% (COD value 0.284). Fitting is illustrated in Figure 7.

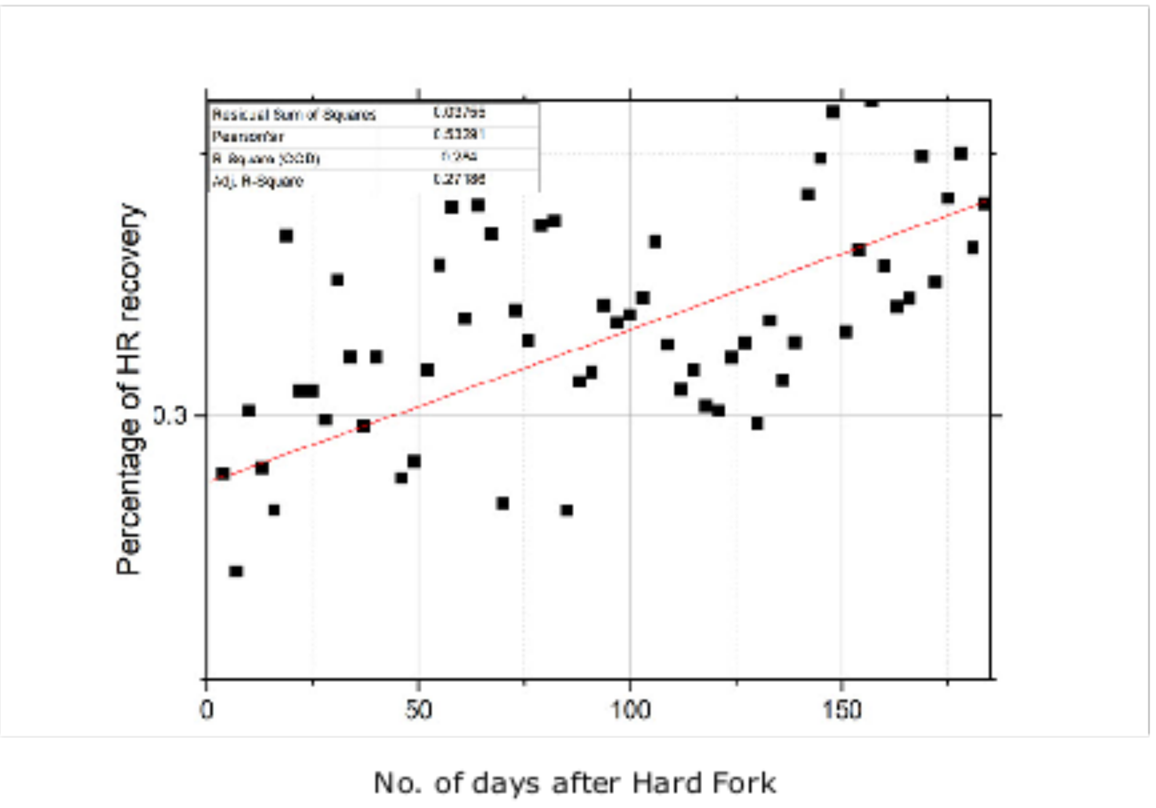

Figure 7. HR trend After V14

This proved the proposed hypothesis H1, namely that the influence of the ASIC machines on the overall HR of system can be calculated and empirically analyzed by symmetrical linear regression models.

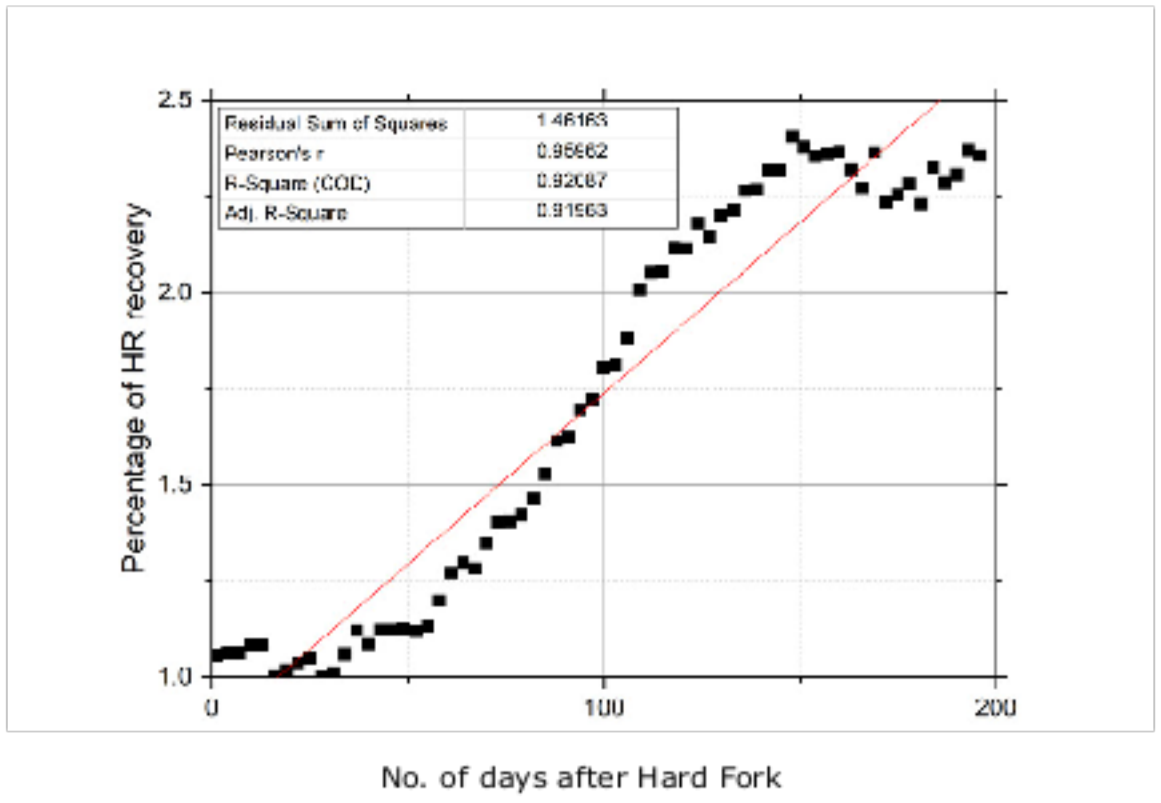

Figure 8. HR trend after Byzantium HF

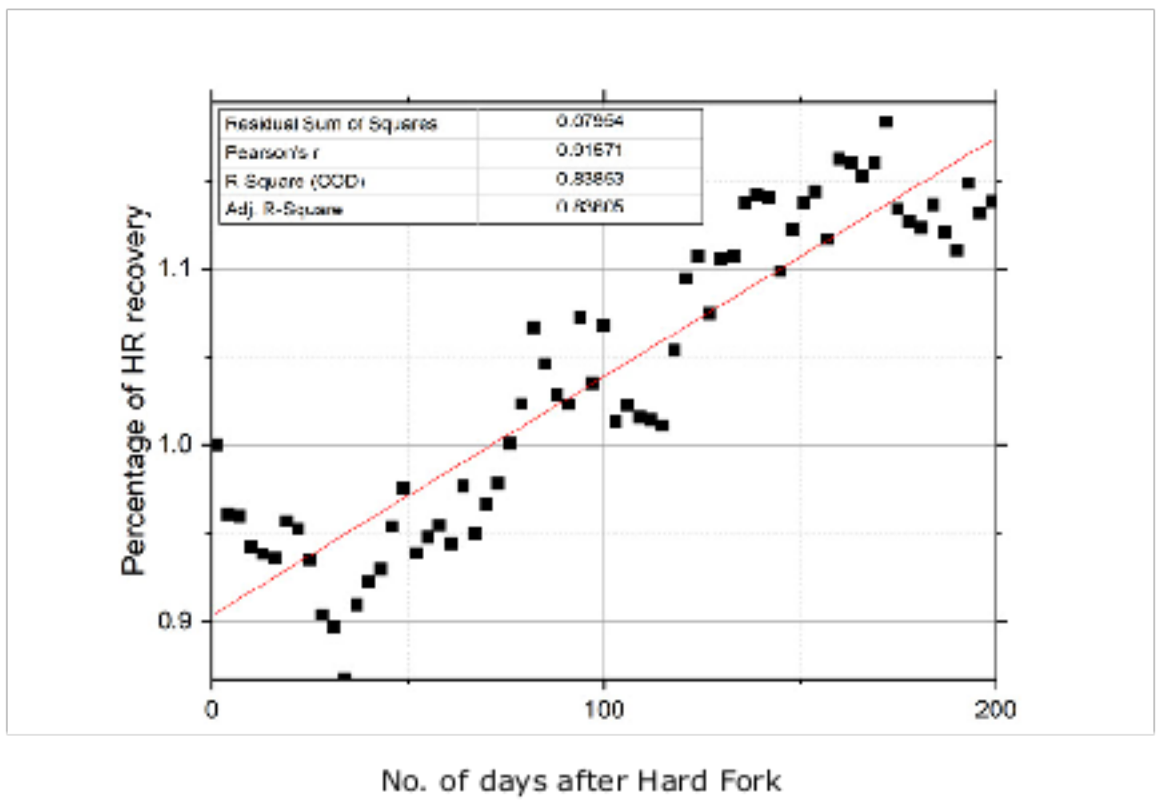

Figure 9. HR trend after Constantinople HF

The second hypothesis (H2) states that Symmetrical regression models and trends of HR change for the systems in which ASICs machine mining is allowed are statistically different from equivalent models in the systems where ASIC machine mining is forbidden.

In order to prove this it was necessary to statistically compare values of the symmetrical linear regression models in which ASIC mining was allowed with models in which this type of mining was prohibited.

First, the symmetrical linear regression model was compared with regard to Monero v.010 and v.011 HFs and Constantinople and Byzantium HFs of Ethereum. It was presumed that ASICs mining happened during the respective period of time and in Ethereum this type of mining was allowed and it was expected that there would be no statistical difference between the two fitting models. One-way ANOVA was used for these models. We will use p-value which is a measure of the probability that an observed difference could have occurred just by random chance. Prob>F is the p-value for the whole model test. In one-way ANOVA if Prob>F is less then 0.05 we will reject null hypothesis, and if greater then 0.05 we will accept null hypothesis. Results in Table 1 show that means are not statistically different at the 0.05 level.

After HFs v.012, v.013 and v.014 there was an active effort to mitigate silent ASICs mining, the three analysed models should not be statistically different. Again, one-way ANOVA was used and it showed that means of the models were not statistically different at the 0.05 level as it can be seen in Table 2.

This analysis showed that systems incorporating ASICs mining have similar statistically symmetrical linear regression trends between themselves. A similar pattern occurred in the systems which required ASICs mining restriction.

For the final conclusion, one statistically compared HR trends after v.012, v.013 and v.014.

HFs with HR trends after v.010, and v.011 HFs and the Constantinople and Byzantium HFs, respectively. Results showed that means of the models were statistically different at the 0.05 level as it can be seen in Table 3.

Further on, the results of the calculations are discussed in line with the research hypotheses. H1 stated that the influence of the ASIC machines

Table 1. Using one-way ANOVA on linear fitted data to show that means of the linear fitted models are not statistically different at the 0.05 level in systems with ASIC machine mining

	Degrees of Freedom (DF)	Sum of Squares	Mean Square	F Value	Prob > F
Model	3	0.00876	0.00292	2.29996	0.15404
Error	8	0.01016	0.00127		
Total	11	0.01892			

Table 2. Using one-way ANOVA to show that means of the linear fitted models are not statistically different at the 0.05 level in systems without ASIC machine mining

HF included in analysis		DF	Sum of Squares	Mean Square	F Value	Prob>F
v.012 v.013 v.014	Model	2	0.0598	0.0299	1.50824	0.29467
	Error	6	0.11894	0.01982		
	Total	8	0.17874			

Table 3. Comparison between HR trends after v.012, v.013 and v.014 HFs with HR trends after v.010 and v.011 HFs and after the Constantinople and Byzantium HFs

HF included in analysis		DF	Sum of Squares	Mean Square	F Value	Prob>F
v.010, v.011, v.012, Const., Byz.	Model	4	0.68371	0.17093	32.04023	1.11997 10^{-5}
	Error	10	0.05335	0.00533		
	Total	14	0.73706			
v.010, v.011, v.013, Const., Byz.	Model	4	0.31867	0.07967	18.74629	1.22072 10^{-4}
	Error	10	0.0425	0.00425		
	Total	14	0.36117			
v.010, v.011, v.014, Const., Byz.	Model	4	0.6935	0.17337	32.36001	1.07017 10^{-5}
	Error	10	0.05358	0.00536		
	Total	14	0.74707			

Table 4. The analysis of the values of the Residual Sum of Squares

	v.010 and v.011	v.011 and v.012	v.012 and v.013	v.013 and v.014	After v.014	After Byzantium release	After Constantinople release
F	303.9204	542.461	25.4372	56.41302	23.40171	744.7720	337.5572
p	0	0	4.13152 10^{-6}	2.34872 10^{-10}	9.8084 10^{-6}	0	9.8084 10^{-6}

on the overall HR of system can be calculated and empirically analyzed by symmetrical linear regression models. Results showed that in the cases when there was no effort in mitigating effects of the ASICs mining, i.e. after HFs v.010 and v.011 and in systems which allow ASICs-based mining, i.e. in Ethereum symmetrical regression models HR change was properly described before and after every HF. The reason for this is increase of the HR which ASIC machines as specialized calculating machines deliver to the Blockchain system. After HF in this type of Blockchain systems, those machines continue to deliver constant HR in the system.

After mitigation effort symmetrical regression models can not cover all calculating power since all the ASIC-based calculation power is, at HF moment cut off from the system and only CPU- and GPU-based calculations are involved.

These results also provided important empirical information on successful implementation of the mitigation effort of the core Blockchain development team and thereby proved H4.

The comparative analysis also showed that there is significant statistical difference between systems in which ASICs mining is allowed and the systems which use CPU-and GPU-based hashing calculations, thereby proving H3.

Finally, the results of the analysis are used for calculating ROI parameter for implementation of silent mining activity as the tool for compromising Blockchain systems. The cost-benefit analysis showed that additional HR was produced by 2393 ASIC machines. Running costs for this type of silent mining operation amounted to 673,000.00 USD for electrical power. The additional research and development cost for ASIC machines amounts to approximately 5,240,670.00 USD (80% of planned selling price). Expected profit from cryptocurrency mining (at the time of the silent mining attack) is 6,640,000.00 USD. The additional profit from machine sales would be 52,650,670.00 USD (it was calculated that the selling price for machines would bring a revenue amounting to 20% of selling price). Final cost-benefit analysis showed that the cost-benefit ratio would be 1:2. This value is much lower than expected cost-benefit ratios for compromising system using CPU- or GPU-based calculating machines.

Change of PoW rendered all these machines obsolete so all planned profit from selling of machines was not delivered. This case showed that attacks and misuse of the Blockchain systems even when plausible still are highly risky actions from a financial point of view.

5. Conclusion

This work provides empirical proofs of silent mining operation in CryptoNight-based Blockchain systems. This action was implemented by using ASIC machines specialized in CryptoNight PoW hash functions. One managed to model systems using linear regression model for HR of the Blockchain systems after distinctive HF. This paper also shows that mitigation of this type of attacks can be easily implemented, so this type of activities are financially risky for entities which want to use them.

Acknowledgments

This paper is part of the research subproject 3 in project no. III 47016, supported by the Ministry of Education, Science and Technological development of the Republic of Serbia.

REFERENCES

Anon (2020a). Available at: <https://bitinfocharts.com/comparison/hashrate-eth-xmr.html>, last accessed: 2nd November, 2021.

Anon (2020b). Available at: <https://bitinfocharts.com/comparison/ethereum-hashrate.html#3y>, last accessed: 2nd November, 2021.

Bevington, P. & Robinson, D. K. (1969). *Data Analysis and Error Analysis for the Physical Sciences.* McGrawe Hill.

Bitmain Technologies Ltd (2018). Available at: <https://twitter.com/BITMAINtech/status/974180147166261248>, last accessed: 2nd November, 2021.

Edwards, A. L. (1976). *An Introduction to Linear Regression and Correlation.* W. H. Freeman & Co, San Francisco, CA.

Fujisaki, E. & Suzuki, K. (2007). Traceable ring signature. In *International Workshop on Public Key Cryptography* (pp. 181-200). Springer, Berlin, Heidelberg.

Gorkhali, A., Li, L. & Shrestha, A. (2020). Blockchain: a literature review, *Journal of Management Analytics*, *7*(3), 321-343.

Kurzweil, R., Richter, R., Kurzweil, R. & Schneider, M. L. (1990). *The Age of Intelligent Machines, vol. 579*. MIT Press, Cambridge, MA.

Mekić, E., Purković, S. & Lekpek, A. (2018). Cost benefit analysis of compromising ledger system based on blockchain technology, *BizInfo (Blace) Journal of Economics, Management and Informatics*, *9*(2), 27-38. DOI: 10.5937/bizinfo1802027M

Rogaway, P. & Shrimpton, T. (2004). Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance. In *International Workshop on Fast Software Encryption* (pp. 371-388). Springer, Berlin, Heidelberg.

van Saberhagen, N. (2013). *Cryptonote v2.0*. Available at: <https://github.com/monero-project/research-lab/blob/master/whitepaper/whitepaper.pdf>, last accessed: 2nd November, 2021.

Vasek, M. & Moore, T. (2015). There's No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams. In *International Conference on Financial Cryptography and Data Security* (pp. 44-61), vol. 8975 of Lecture Notes in Computer Science. Springer Berlin Heidelberg.

Vasek, M., Thornton, M. & Moore, T. (2014). Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem. In *International Conference on Financial Cryptography and Data Security,* part of *Lecture Notes in Computer Science*, *8438* (pp. 57-71). Springer, Berlin, Heidelberg.

Williams-Grut, O. (2018). *Business Insider*. Available at: <https://www.businessinsider.com/chinese-bitcoin-mining-bitmain-revenues-ipo-filing-hong-kong-profits-2018-9>.

Zyskind, G., Nathan, O. & Pentland, A. (2015). *Decentralizing privacy: Using block chain to protect personal data.* In 2015 IEEE Security and Privacy Workshops (pp. 180-184).