Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Quantitative Analysis of Cryptocurrency Susceptibility: A Mathematical Benchmarking Model

Ayman Mohammad Bekiroğlu [1*]

[1] *Assistant Professor, Department of Economics, Ibn Haldun University, Istanbul, Turkiye*

[*] *Corresponding Author: ayman.bekiroglu@ihu.edu.tr*

ARTICLE INFO

Received: 30 Dec 2024

Revised: 19 Feb 2025

Accepted: 27 Feb 2025

ABSTRACT

The rise of cryptocurrencies has brought attention to significant security challenges, particularly the 51% attack. This study focuses on developing benchmarks to evaluate varying levels of vulnerability among cryptocurrencies. A detailed review of the literature identifies a lack of approaches having statistical rigor, leading to the development of a comprehensive susceptibility test model. The proposed model is basedonkey parameters extracted from existing studies and validated with additional quantitative data for accuracy and reliability. Benchmarking thresholds are determined using k-means clustering, allowing for the classification of cryptocurrencies into distinct security profiles. The analysis identifies five clusters: resilient cryptocurrencies have susceptibility scores below 0.532, while scores exceeding 1.557 indicate high vulnerability. The remaining clusters represent intermediate levels of resilience and risk. These findings contribute to a better understanding of cryptocurrency security, supporting informed investment decisions and providing a basis for future research and policy development.

Keywords: Cryptocurrency . Security Majority Attack . Informed investment decisions . Susceptibility Test Model . Mathematical Modeling . K-means Clustering

1. INTRODUCTION

Because of their innovative features, cryptocurrencies have piqued the curiosity of various individuals, such as economists, researchers, developers, investors, and technologists. They possess remarkable attributes that hold the potential to catalyze a revolutionary transformation in the digital realm. This is evident in the groundbreaking encryption and tokenization capabilities provided by their underlying blockchain technology, which enables trading without intermediaries (Maghdeed 2020a).

The decentralized aspect of cryptocurrencies is especially notable in light of the 2007 financial crisis and the COVID-19 pandemic. These events exposed weaknesses in traditional financial systems, leading many to seek alternative methods for transferring funds securely. Cryptocurrencies provide an exciting new possibility for transferring funds quickly, reliably, and securely without traditional intermediaries like banks, credit cards, and payment gateways (Maghdeed 2020b). As a result, there has been a consistent uptick in the popularity and use of cryptocurrencies, posing a significant challenge to these traditional financial systems and institutions.

Although the adoption of cryptocurrencies initially began with individuals and some merchants, large corporations and governments have increasingly accepted these virtual currencies. For example, Microsoft now accepts Bitcoin as payment in its stores. Also, Tesla Corporation was previously accepting Bitcoin from customers in exchange for Tesla vehicles (Novet 2022). The US Department of Treasury's Financial Crimes Enforcement Network (FinCEN) considers "convertible" virtual currencies either having an equivalent value in real currency or acting as a substitute for real currency (FinCEN 2013). The Internal Revenue Service (IRS) treats virtual currencies as properties for taxation purposes (IRS 2014). Other entities, like the Canada Revenue Agency (CRA) and the Australian Taxation Office (ATO), have similar treatments (ATO 2023; CRA 2023). On the other hand, second only to El Salvador, the Central African Republic recently made bitcoin a legal tender (Browne 2022).

Despite these advantages, cryptocurrencies are not immune to security threats. A major security concern of blockchain based system is the 51% attack (Zhao, Fan, & Yan 2016). This type of attack occurs when an entity gains control of the majority of a cryptocurrency's mining power, thereby allowing them to manipulate transaction records

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

and potentially double-spend coins. The ramifications of such an attack can be very devastating, triggering waves of loss of trust in the cryptocurrency.

The longstanding assumption was that such an attack would be unlikely due to its high cost, discouraging potential attackers. However, this long-held belief failed to stand as many cases of 51% attacks have been detected. Yet, in case of collusion the stability remains undetermined. For example, in July 2014, the hash power of the Bitcoin network was briefly dominated by GHash.IO, a popular Bitcoin mining pool, exceeding 50% control (Bonneauetal. 2015). In response to concerns about a possible attack, the pool publicly pledged to limit its future capacity to avoid undermining confidence in the system. It is important to mention that there hasn't been any indication of a harmful mining attack on the Bitcoin network.

In contrast, numerous smaller cryptocurrencies with lower market capitalization and network size have fallen victim to 51% attacks. The system developed by the Digital Currency Initiative (DCI) has detected over 40 chain reorganizations that were 6 or more blocks deep in several proof-of-work (PoW) cryptocurrencies, including bitcoin gold (BTG), verge (XVG), and light-coin cash (LCC) (DCI 2020). Some of these attacks came from hash rental sites. This clearly indicates that 51% attacks can have a significant impact on the network.

Therefore, it is commonly believed that smaller networks are more susceptible to 51% attacks, while larger networks are more resilient. Numerous studies have suggested that cryptocurrencies with high network hashing are more secure against 51% attacks compared to those with lower network hashing. For example, in his study, Courtois (2014) showed that smaller altcoins are substantially more vulnerable than Bitcoin. Furthermore, 51% attacks are primarily characteristic of small PoW cryptocurrencies with low hash rate (Shanaev, Shuraeva, Vasenin, & Kuznetsov 2020). This vulnerability becomes even more pronounced when higher hashing power is abundantly available for rent, as observed by Yang, Chen, & Chen (2019), who note that the cost of creating a 51% attack can become surprisingly low. Likewise, Sayeed & Marco-Gisbert (2019) maintained that cryptocurrencies with a higher level of network hashing are more resilient. A separate analysis also revealed that short selling attacks pose a larger threat to smaller-scale chains (Zhang, Yang, Chen, & Xue 2022).

The analysis of cryptocurrencies' risk exposure has been proven difficult for both investors and researchers (Ramos, Pianese, Leach, & Oliveras 2021; Shanaev et al. 2020). Information like rentals of large hash power is not easily accessible nor readily deducible by stakeholders such as investors and researchers. Additionally, The literature does not distinctly delineate a spectrum encompassing the varying degrees of vulnerability and resilience among cryptocurrencies concerning their susceptibility to 51% attacks; rather, the available information must be carefully curated and processed in order to draw meaningful conclusions. We, therefore, believe that establishing such a threshold is crucial, as it will guide various stakeholders including cryptocurrency developers in ensuring the long-term reliability and security of the system, Islamic economists and jurists in determining the Sharīʿah compliance of the cryptocurrency, and investors in managing their investment portfolios. This study aims to bridge this gap by developing and benchmarking a susceptibility test.

In addition to this introduction, the remaining of the study is divided into four other sections. Section two provides a literature review, which explores the current understanding of vulnerable and resilient cryptocurrencies. Section three details the methodology used to establish the threshold for 51% attack susceptibility. Section four presents the results and findings. Section five is the conclusion, which summarizes the main findings.

2. RELATED LITERATURE

Due to being widely acknowledged as a critical vulnerability in blockchain systems, it has been suggested that 51% attacks represent significant risks for investors in cryptocurrencies (Shanaevetal. 2020). Although 51% attacks pose a threat to both PoS and PoW networks, they are particularly risky for the attackers on PoS networks (Dusart 2023). A reliable indicator of a potential 51% threat in PoS systems is the awareness of a substantial stake nearing the 50% mark—an advantage not easily attainable in PoW networks, where such information is more obscure. Although much research has been conducted on the impact and mitigation of these attacks, a gap remains in developing a unified model that integrates various parameters to assess vulnerability systematically. This review critically engages with the existing literature, highlighting the interplay between different studies, and identifies the key parameters to be adopted in the present study.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

König, Unger, Kieseberg, & Tjoa (2020) and Ramos et al. (2021) offered foundational insights into the risks posed by 51% attacks, with the latter extending the analysis to their economic impact. While König et al. provided a broad overview, Ramos et al. delved deeper, revealing a consistent negative effect on cryptocurrency returns, a finding echoed by Mrazek et al. (2022). These studies underscore the pervasive threat of 51% attacks, yet their primary focus remains on the symptoms rather than the underlying vulnerabilities that exacerbate these attacks. In contrast, Zhang et al. (2022) addressed these vulnerabilities by introducing the concept of 51% attacks in the context of short selling, particularly highlighting their severity in smaller blockchains. Zhang's work, however, stops short of proposing concrete countermeasures, leaving a gap that subsequent research attempts to fill.

A cohort of researchers primarily focused on proposing and evaluating countermeasures against 51% attacks. Conti, Kumar, Lal, & Ruj (2018) and Sayeed & Marco-Gisbert (2019) represented two key approaches: the former emphasized identifying vulnerabilities within Bitcoin's PoW framework while also devoting considerable effort to investigating the feasibility and robustness of the latest security solutions, while the latter provided a critical evaluation of the five most advanced protection techniques. Both studies contribute significantly to understanding the strengths and limitations of current security measures, but they were limited to assessing risks of one consensus mechanism. Guo & Yu (2022) attempted to bridge this gap by offering a comparative analysis across different consensus mechanisms, though their focus remains on summarizing rather than integrating these into a cohesive model indicative of vulnerabilities. Similarly, Hasanova, Baek, Shin, Cho, & Kim (2019) and Li et al. (2020) contributed to this discourse by cataloging potential countermeasures, but their work largely remains descriptive, lacking the analytical depth needed to inform practical applications and required parameters for developing indicators of attacks.

The technical intricacies of countermeasures become more apparent in the work of Yang et al. (2019) and Duong et al. (2020). Yang et al. proposed a scheme, called PoW based on historical weighted difficulty (HWD-PoW), which uses the frequency rate of miners in historical blocks and calculates the total weighted historical difficulty to examine whether a branch change is necessary. Yang's proposal, while innovative, reveals significant limitations, particularly in its inability to address gradual hashrate increases. Duong's 2-hop blockchain, which combines PoW with PoS, offers a more robust solution but at the cost of increased centralization—a trade-off that could undermine the very principles of decentralization that blockchain seeks to uphold. In fact, the 2-hop blockchain countermeasure hasn't seen wide acceptance and was only adopted by TwinsCoin (Aponte-Novoa et al. 2021). Similar to the previous solution, Niranjani et al. (2022) advocated for a hybrid PoW-PoS reward system for a newly starting crypto, with no sufficient network and resource distribution, incorporating miner selection randomization to enhance resistance to 51% attacks. However, this approach as well faces challenges, notably in its potential to determiner participation due to its financial unattractiveness. These studies collectively highlight the significance of hashrate parameters as critical guage of security and highlight the complexity of developing a one-size-fits-all solution, suggesting that any effective model must be both adaptable and sensitive to the specific context of each blockchain network and its size.

Building on the challenges identified in traditional blockchain mechanisms, the exploration of artificial intelligence (AI) introduces a novel dimension to enhancing blockchain security. Dey (2018) and Scicchitano et al. (2020) represent two key studies in this area, with Dey proposing a supervised machine learning approach and Scicchitano favoring an unsupervised sequence-to-sequence neural network model. Dey coupled supervised machine learning with algorithmic game theory to develop intelligent software agents capable of detecting stakeholder anomalies, such as collusion. In case collusion was detected, the algorithm will not pass the new block for validation, thus eliminating 51% attacks; rather, it will return for a new round of finding the next block. On the other hand, Scicchitano et al. employed artificial intelligence via a sequence-to-sequence neural network model to recognize anomalous changes in the blockchain network. While both approaches show promise, they are not without their drawbacks—according to Aponte-Novoa et al. (2021), Dey's method has been criticized for its inability to accurately assess product importance, and Scicchitano's model suffers from false detections. These issues underscore the importance of integrating AI with other methodologies to enhance accuracy and reliability, rather than relying on it as a standalone solution.

In order to avoid the disadvantages and inherent issues of classical blockchains and the limitations of the proposed security measures discussed earlier, several studies proposed various quantum signature schemes instead. In a

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

previous study by Wen et al. (2022), they suggested using quantum blockchain consensus mechanism. The rationale for doing so is that with quantum consensus, no computational power is required while randomness of miners is ensured by the irreversibility of quantum measurement and quantum zero-knowledge proofs. However, in their most recent study, Wen et al. (2022) admitted that their previous proposal is complicated and hard to realize. In their new scheme they suggested quantum cryptography which ensures randomness of miners using quantum teleportation and quantum measurement. Despite their new scheme, their proposal is yet to be analyzed in terms of complication and degree of difficulty to implement.

As discussed above, while certain security measures and proposals have been implemented, their application has often been restricted to specific blockchains or has demonstrated inadequacy. Moreover, several of these initiatives have remained at the prototype stage, while many others are still confined to ongoing academic discussions and studies. Accordingly, devising an indicator that can detect the susceptibility degree of a PoW crypto to 51% attacks remains significant. The author is aware of one study only, conducted by Lansky (2020), that focused on providing such an indicator for PoW networks. The study provided a practical benchmark for these stakeholders by analyzing over 2,500 cryptocurrencies. He found that 70 percent of those delisted from exchanges did so within their first year, while cryptocurrencies with five years of trading history have a low probability of 9 percent to be delisted from exchanges within a year. Based on these findings, the author recommends investors wait at least one year before investing in a new cryptocurrency and suggests a five-year waiting period for maximum security. While Lansky's wait period is a general investment indicator based on statistical analysis, it can be overly cautious and lead investors to miss opportunities, such as investing in a cryptocurrency at a low cost during its early years.

Building on Lansky's approach, the present study seeks to devise benchmarks that not only indicate the safety of cryptocurrencies but also assess their vulnerability levels with greater precision. This will be achieved through a more comprehensive data analysis that incorporates critical parameters identified in the literature, particularly network hashrates.

The reviewed security measures, despite their importance, have shown limitations in fully safeguarding against 51% attacks. However, the literature highlights hashrates as a crucial parameter for determining the security of PoW networks, and this will be a key component in the model proposed by this study. This model is believed to be more robust since it promises to expose the true risk level of each cryptocurrency and is hoped to be better than the general five-year wait period suggested by Lansky (2020), since it will avoid missing investment opportunities.

3. METHODOLOGY

As discussed, one of the gaps identified from the extant literature is the lack of a susceptibility model based on hashrates which makes cryptocurrency susceptibility values unavailable. Therefore, with the absence of such values, traditional multiple regression is unsuitable for identifying effective factors and achieving the best fit. On the other hand, mathematical models offer new possibilities to manage the increasing complexity of technology (Quarteroni 2009). Thus, to address the former limitation, this study adopted a mathematical modeling approach to develop a susceptibility test model based on essential parameters obtained from the literature.

3.1 Data Selection and Sampling

In this study, stratified random sampling was used to acquire a cross-sectional snapshot of data. PoW cryptocurrencies were identified into three strata according to their network hashrates (computational power). They were randomly selected from WhatToMine (2023) and Profit-mine (2023) during April 2023, provided the required information such as network hashrate, block reward, and algorithm were available. The sample size encompassed 55 observations: 11 having net hashrate greater than 1 Penta Hashes per second, 28 between 1 Giga and 1 Penta Hashes per second, and 16 less than 1 Giga Hashes per second. These represented a diverse array of PoW algorithms: SHA-256, Scrypt, Zhash, X11, X13, NeoScrypt, Etchash, BeamV3, Blake2s, Equihash, Lyra2Rev2, CuckooCycle, KHeavyHash, RandomX, and KawPow.

3.2 Parameters

As discussed in the first section and the literature, several studies pointed out that the size of the network matters in terms of vulnerability to attacks (Courtois 2014; Sayeed & Marco-Gisbert 2019; Shanaev et al. 2020; Zhang et al.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

2022). As such, network hashrate was considered one of the main parameters to be extracted. On the other hand, abundance of rented hash power and cost of attack are identified as two more parameters to be considered (Yang et al. 2019) with a general assumption that the motivation behind 51% attacks is monetary in nature. Therefore, block reward made a fourth extractable data. Notably, other intentions of 51% attacks are also possible, such as political or sabotage. However, this study assumes that 51% attacks are driven by the reward the attacker will gain. Therefore, the parameters used in the model encompassed the mean price in dollars paid for hashrate renting per day and the available hashrate for renting for each PoW algorithm. These cross-sectional data were manually captured from NiceHash (2023) between April 19th and May 2nd, 2023. Additionally, the network hashrate and block reward were manually obtained from WhatToMine (2023) and Profit-mine (2023) during the same time period.

3.3 Preprocessing

The extracted network hashrates were in different units depending on the size of the network. For example, Bitcoin with algorithm SHA-256 was given in Exa Hashes per second (that is 10 to the power of 18) while Dogecoin with algorithm Scrypt was given in Tera Hashes per second (10 to the power of 12). Accordingly, network hashrate size was standardized to the unit of hashes per second (H/s). Similarly, the mean, max, and total rent rate units differed for each algorithm. These were also standardized to the unit of H/s.

Conversely, the price extracted from NiceHash (2023) was originally quoted in bitcoins per network hashrate unit per day. To standardize this, the price was converted to US dollars using the Bitcoin to USD exchange rate from May 2, 2023, as provided by CoinMarketCap (2023). According to NiceHash (2023), the rented hashrate order is not executed instantaneously and may take several days contingent upon the specified timeframe. Although the price is quoted on a daily basis, the actual duration of the attack might last only a few hours. Therefore, the price was divided by 24 to accurately reflect the hourly cost for the effective attack.

Lastly, this study preferred to employ the total rent hashrate instead of the mean rent hashrate for the following reasons. The rent hashrate drawn from NiceHash (2023) is a spot capture of a dynamic data. Since NiceHash (2023) doesn't continuously deliver hashrates, the captured dataset contains numerous zeros for rented hashrates. This might change depending on the moment it was captured. Incorporating these zeros in the calculation of the mean would skew the distribution to the left (Larson & Farber 2019). Conversely, omitting them risks losing important data associated with the hashrates, such as the price paid (NiceHash 2023). Again, this is because hashrate is dynamic and varies over time. Secondly, the total rented hashrate in the sample represents the maximum realistically attainable hashrate according to NiceHash (2023).

3.4 Approach

The mathematical model was built based on the literature using the parameters discussed above. The rationale is to use the model to describe the different aspects [vulnerability in this study] of the real world [cryptocurrencies] through mathematics (Quarteroni 2009). The model was then subjected to statistical analysis and further refined, aided by visual plots. Subsequently, it was validated against cryptocurrencies outside the sample to ensure its efficacy, reliability, and robustness.

In order to assess the vulnerability levels of cryptocurrencies and establish benchmarks, a technique was required to group similar data points together. Achieving this aim facilitated the application of clustering, a machine-learning technique designed to delineate and easily analyze these distinctive groupings (Omardonia 2023). Our dataset was one-dimensional and involved the calculation of numerical susceptibility values for 55 observations. Hence, according to Omardonia (2023), k-means clustering makes a good clustering technique for numerical data. The k-means algorithm iteratively assigns data points to the cluster whose centroid is closest, typically measured using the Euclidean distance metric (Omardonia 2023). After assigning all data points, the centroids are updated by calculating the mean values of the data points within each cluster. This iteration continues until convergence is achieved. Relational clustering techniques like hierarchical clustering and agnes were excluded because no relationship between the dataset values was required for the purpose of this study. Furthermore, several clustering algorithms, such as optics and dbscan, could obtain different results for non-normally distributed data (Rodriguez et al. 2019). In this study, procedures were taken to normalize the data via taking a logarithmic scale, and therefore, the study preferred to work only with k-means clustering.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The data was pre-processed and normalized to ensure consistency and suitability for analysis. Pre-processing involved normalizing the data with logarithmic scales. Moreover, the model's calculated susceptibility values were standardized by taking their z-scores. No outliers were found. A good strategy to choose k is to set it to values slightly higher than the expected number of classes (Rodriguez et al. 2019). Hence, to determine the appropriate number of clusters, we started with a high number using R statistics and iteratively tested different k values. We also conducted a screeplot for which an elbow, point of inflection, can indicate the number of significant factors to retain. Figure 1 illustrates a scree plot representing the within-cluster sum of squares (WSS) results plotted against the number of clusters employed. The objective is to minimize the WSS. As the number of clusters increases, the WSS value decreases, each time at a slower rate. The scree plot reveals a distinct elbow point at 5 clusters, beyond which the improvement in WSS becomes significantly negligible as the rate of change is conspicuously slower. Moreover, the average silhouette for 5 clusters was found to be 0.6246461. This indicates that the clusters were well-defined and well-separated from each other (Ozturk 2023), a sign that the choice of 5 clusters was good.

The resulting clusters were evaluated and interpreted by analyzing the characteristics and patterns within each cluster. Furthermore, cluster evaluation metrics were employed to assess cluster compactness, separation, and coherence. The Dunn Index was used to measure the compactness and separability of the clusters with a high number indicating a better clustering solution (Ozturk 2023). On the other hand, a commonly used evaluation metric, Calinski-Harabasz, was employed to measure the between-cluster variance and the within-cluster variance (Ozturk 2023).

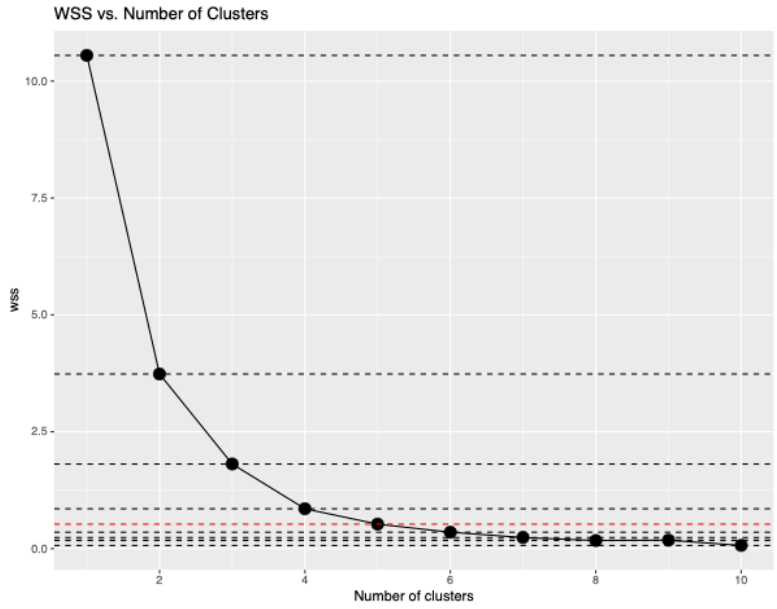

Figure 1. Screeplot showing WSS results against the number of clusters used.

The higher the number, the better is the clustering performed. Lastly, Davies-Bouldin metric was utilized to measure the similarity between the clusters (Ozturk 2023) with lower values implying dissimilar clusters and thus a better cluster solution. Based on the cluster analysis results, specific thresholds can be established to differentiate vulnerability levels, thus categorizing cryptocurrencies as extremely vulnerable, highly vulnerable, moderately vulnerable, moderately resilient, or resilient.

4. FINDINGS AND ANALYSIS

This section provides the findings in two main subsections. The first subsection introduces and analyzes the model developed through the process of mathematical modeling. The second subsection evaluates the model using the

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

sample data to establish benchmarks, enabling a spectrum of differentiation between resilient and non-resilient cryptocurrencies.

4.1 Mathematical Modeling of the Susceptibility Test

This subsection delves into the process of developing the susceptibility test model using mathematical modeling which consists of five fundamental steps. Firstly, the scope of the problem is defined, outlining the key aspects to be addressed. Next, the model is formulated by carefully selecting and incorporating essential parameters. Subsequently, the computation of susceptibility test values takes place, utilizing the model to assess the vulnerability levels of cryptocurrencies. The interpretation of these results follows, shedding light on the underlying patterns and characteristics of the data. Lastly, the model undergoes validation, ensuring its efficacy, reliability, and robustness against external data.

4.1.1 Scope of the Problem

PoW-based virtual currencies are particularly susceptible to 51% majority attacks (Dusart 2023; Nguyen et al. 2019). While some PoW cryptos have demonstrated resilience against these attacks, others have suffered significant losses in the order of millions of dollars. Therefore, the question arises: can a test indicator be developed to distinguish the degree of resilience of PoW cryptos?

4.1.2 Formulating the Model

Numerous studies have suggested that cryptocurrencies with high network hashing are more secure against 51% attacks compared to those with lower network hashing (Courtois 2014; Sayeed & Marco-Gisbert 2019). Similarly, other studies asserted that 51% attacks are primarily characteristic of small PoW cryptocurrencies with low hash rate (Shanaevetal. 2020; Zhang et al. 2022). Therefore, in a PoW cryptocurrency, the larger the network's hashrate, the more nodes you will have to dominate in order to control 51 percent of it. The difficulty increases many folds and therefore a large cryptocurrency network is less susceptible to attacks. This indicates that the susceptibility to attacks is inversely proportional to the network hashrate.

Let the susceptibility test and the total network's hashrate be s and n respectively. Therefore, $s \propto 1/n$. On the other hand, the vulnerability becomes even more pronounced when higher hashing power is abundantly available for rent (Yang et al. 2019). As such, the higher the availability of rented hashrates in the market, the more one can control of the intended cryptocurrency network. If the rented hashrate is sufficient to control the majority of the network's hashrate, then theoretically it becomes easy to carry out 51% attacks. So, susceptibility to attacks is directly proportional to the rented hashrate, that is $s \propto h$, where h is the total rented hashrate available in the market.

However, the cost of renting hashrates from the market or cost of hardware required to control the majority of the network will act as a deterrent to attacks even if the available hashrate rental is abundant. It follows then that $s \propto 1/c$, where c represents the theoretical cost of renting hashrate for one hour attack, refer to subsection 3.3. We assume that $c > 0$ as any attack should always incur costs. Any value less than one would weaken the network's hashrate, ultimately resulting in an increase in s. This is contrary to the intended purpose, as incurring a cost is meant to act as a deterrent to attacks, which should lead to a decrease in s. However, this can be tolerated and assumed that a cost less than one dollar is very affordable which encourages attacks. Therefore, we propose the following formula for the susceptibility test:

$$s = \frac{h}{c \cdot n}, \quad c > 0 \qquad (1)$$

where,

$$c = 0.51n \cdot \frac{P_\mu}{24}$$

is the theoretical cost of one hour attack and P_μ is the mean price in dollars paid for hashrate renting per day (because the amount of hashrate rented from NiceHash (2023) is given per day); hence, to get the cost of one hour, it is divided

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

by 24. To control 51 percent of the network, the mean price is multiplied by 51 percent of the network's hashrate. However, despite the cost incurred, an attacker will be driven by the rewards gained from the attack. If a majority attack is successful, the cost will decrease and in some cases turn into profits. Assuming the reward gained to be one block reward, the model in equation 1 can be improved as follows:

$$s = \frac{h}{n \cdot |c-r|^{\frac{c-r}{|c-r|}}}, \quad |c-r| > 0 \qquad (2)$$

where r represents one block reward. Equation 2 incorporates a more realistic cost where it is reduced by the amount of block reward gained. The absolute value around $c-r$ ensures that s never becomes negative. However, when $c-r<0$, the attacker will have achieved a profit and, therefore, this multiplying factor should no longer reinforce the network's hashrate in the denominator. Instead, the factor should be reinforcing to increase the susceptibility value; as such, the multiplying factor should multiply the numerator, or the total rented hashrate. The power $(c-r)/|c-r|$ ensures that this purpose is achieved. When $c-r>0$, the power $\frac{c-r}{|c-r|} \to 1$ and the factor multiplies the denominator.

In converse, when $c-r<0$, the power $\frac{c-r}{|c-r|} \to -1$ and the factor multiplies the numerator. The condition $c-r>0$ is necessary to ensure that the equation doesn't divide by zero. If $|c-r|=0$, the cost c and block reward r are equal, and in this case we can set the value to 1 so that the determining factor for susceptibility becomes the highest of n or h.

The above models in equations 1 and 2 have several assumptions. First, the models do not consider future technological development which can become a significant factor in the equation. Technology advancement from the mining side can potentially undermine a cryptocurrency's network and increase its susceptibility to attacks. On the other hand, technology development in a crypto's network can play a major role in increasing its security and reducing its vulnerability to attacks. Second, it is also assumed that the total rented hashrate data is representa tive of the total rented hashrate in existence. Furthermore, the cost-only model in equation 1 does not consider the rewards for successful attacks which can significantly reduce the cost. Nonetheless, equation 2 adds this factor to it. But it assumes that, on a successful majority attack, the attacker will gain only one block reward. In reality, the attacker can make many more reorgs, potentially double-spending with several block rewards. Yet, in order to do so, the attacker might require more than one hour attack, and thus we assume that a one block reward is balanced by the cost incurred in one hour attack. Third, the second model assumes that the motivation for the attack is monetary in nature. Other reasons exist, such as political and sabotage intentions, which can be more explained with the first model.

4.1.3 Computing the Susceptibility Test

Equations 1 and 2 suggest that a cryptocurrency's susceptibility to attacks rises with an increase in the value of s. All other factors being equal, if the total hashrate that is available for rent exceeds 50 percent of the network's hashrate, the cryptocurrency becomes vulnerable to 51% majority attacks, and $s \geq 0.51$. As such, theoretically we expect a cryptocurrency to possess an s value that is less than 0.51 for resilience. To calculate the susceptibility test for each cryptocurrency in our sample, we employed equations 1 and 2, and the results of some of them are presented in Table 1.

4.1.4 Interpretation

Specifically, we expect that the cryptocurrency with the largest network hashrate, relatively lower hashrate rental, and highest cost per one hour attack would exhibit the lowest susceptibility test value. In our sample, Bitcoin possessed the highest cost of hour attack, exceeding 765k per hour, and the largest network hashrate of approximately 438 EH/s[1].

Our susceptibility equations generated a minimum value of almost zero for Bitcoin using both the cost-only model and the cost-reward model. Conversely, the smallest network's hashrate in our sample belonged to BitTubeCash at 474 H/s.

[1] EH, Exa-Hashes, is of the order of 10^{18} hashes

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 1. Calculated *s* value for a selection of the sample

Crypto	Code	Total Rent Hash H/s [a]	Net Hash H/s [a]	Cost $/h [b]	*S* Cost-Only	*S* Cost-Reward
Bitcoin	BTC	1.47800e+17	4.37695e+20	765434.3	4.411588e-10	5.660253e-10
Beam	BEAM	1.86400e+05	2.88500e+05	45.91243	0.01407245	0.01447253
.						
.						
.						
Bitcoin Z	BTCZ	6.18600e+05	9.82300e+04	6.862904	0.9176093	1.006161
Verge	XVG	1.50000e+12	9.78000e+12	0.1628868	0.9416001	1.013254
Gemlink	GLINK	6.18600e+05	1.50700e+04	1.052876	38.98698	42.10103
Hush	HUSH	9.92800e+08	1.04100e+07	2.353372	40.52476	42.14934
BitTubeCash	TUBE	5.43123e+04	4.74000e+02	0.3773113	303.6827	309.7879
Litecoin Cash	LCC	1.47800e+17	4.29600e+14	0.7512779	457.9410	519.9474
Veil	VEIL	1.47800e+17	3.90000e+09	6.820261e-06	5.556596e+12	1382998

[a] H/s = Hashes per second

[b] $/h = Cost of 1 hour attack in dollars

With abundance of rented hashrate that was approximately 100 times larger than its network's hashrate at about 54 KH/s and a relatively low cost of approximately 37 cents, it exhibited a significant susceptibility test value of 303.68 in the cost-only model, and 309.79 in the cost-reward model. In the same vein, Veil, which is the cheapest cryptocurrency to attack with a cost of 0.0000068 per hour, had an extremely high susceptibility value of 5.556596e+12 in the cost-model, and 1,382,998 in the cost-reward model. The very low cost of available rented hashrate was compounded by the staggering difference between it and the network hashrate, which exceeded it by 108 order of magnitude. These factors contributed to the observed phenomenon and the results support our reasoning that susceptible cryptocurrencies tend to have $s \geq 0.51$. However, there are a couple of things worth discussing.

First, the threshold for susceptibility $s \geq 0.51$ is deduced from the total rented hashrate to network hashrate ratio with no consideration to the effect of cost and/or reward. Thus, a more realistic threshold will follow in section 4.2. Second, the cost-reward model, to some extent, relatively gave higher *s* values except for Veil where it had a lower *s* value than in the cost-only model; yet the values in both models are very high that the difference has no significant interpretation.

4.1.5 Validating the Model

The summary statistics for the calculated *s* in both the cost-only and cost-reward models are shown in Table 2. The summary statistics show that there is a large gap between the median and the mean, and that the range is very large in both the models. In fact, the variance is so large in excess of 5.61e+23 in the cost-only model and about 6.91e+10 in the cost-reward model. The standard deviations are about 7.49e+11 and 262794.3 respectively. What is of particular importance is that the mean is greater than the median and exists within the top 25 percent of the data

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

since it falls beyond the 3rd quartile. This means that the statistic is heavily skewed to the right and data tends to be concentrated in the lower part.

Table 2. Summary statistics of s in both the cost-only and cost-reward models

Min	Q1	Median	Mean	Q3	Max
≈ 0[a]	≈ 0[a]	1[a]	1.011e+11[a]	683[a]	5.557e+12[a]
≈ 0[b]	≈ 0[b]	0.6[b]	64125.1[b]	233.7[b]	1.383e+06[b]

[a] S Cost-Only Model
[b] S Cost-Reward Model

Figure 2 further clarifies the issue with box-plot and histogram diagrams. The box-plot in both models suggest several outliers at the extreme right. These box-plots were plotted with logarithmic scale in order to show a comparable box with a clear width. The outliers refer to cryptocurrencies that have significantly poor performance, such as Veil, which was discussed in the previous subsection. However, the cost-reward model seems to accommodate the cryptocurrency sample better than the cost-only model as the former had only six outliers (Figure 2.c) compared to the ten outliers in the latter case (Figure 2.a). In order to have meaningful histograms, these outliers were temporarily removed prior to plotting the diagrams. The resulting histograms, Figure 2.b and 2.d, both support our conclusion that the data is concentrated in the lower part while they clearly show the extent to which the plots are heavily skewed to the right.

These findings and discussions show that a logarithmic scale is required to bring the values to comparable scale and perhaps transform skewed data to approximately conform to normality. Taking the log of the susceptibility test is problematic since it can assume a value less than one and, therefore, cause a negative result. Instead, it would be more logical to apply the logarithm function on each factor under both equations 1 and 2. Notwithstanding, since c under equation 1 and $|c - r|$ in equation 2 can both assume a value less than one, then a logarithmic scale for these factors, c and $|c - r|$, might not be appropriate. We therefore suggest applying an nth root radical to solve that problem. Within the sample's cost per hour attack data range, the closest root is the 5th root as can be seen in Figure 3.

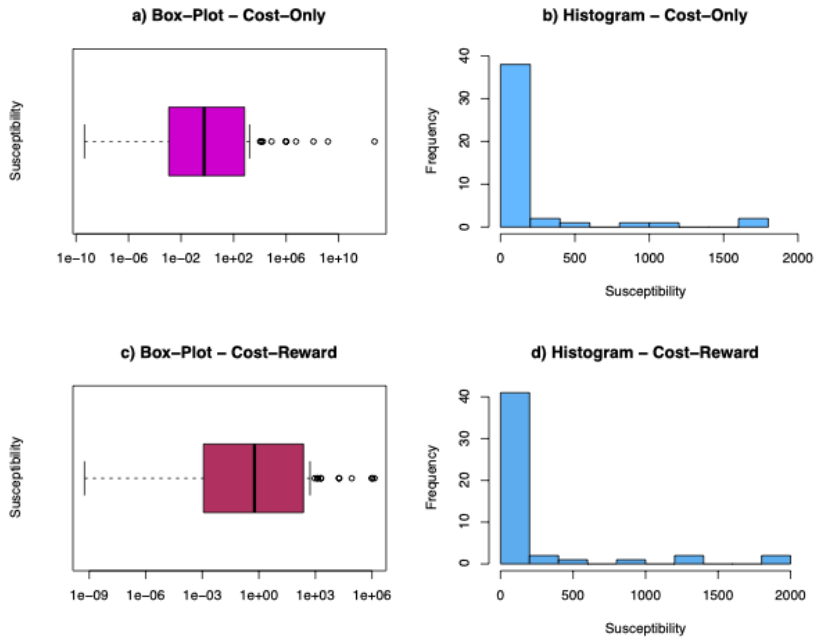

Figure 2. Histograms and boxplots of the susceptibility test in the cost-only and cost reward models

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

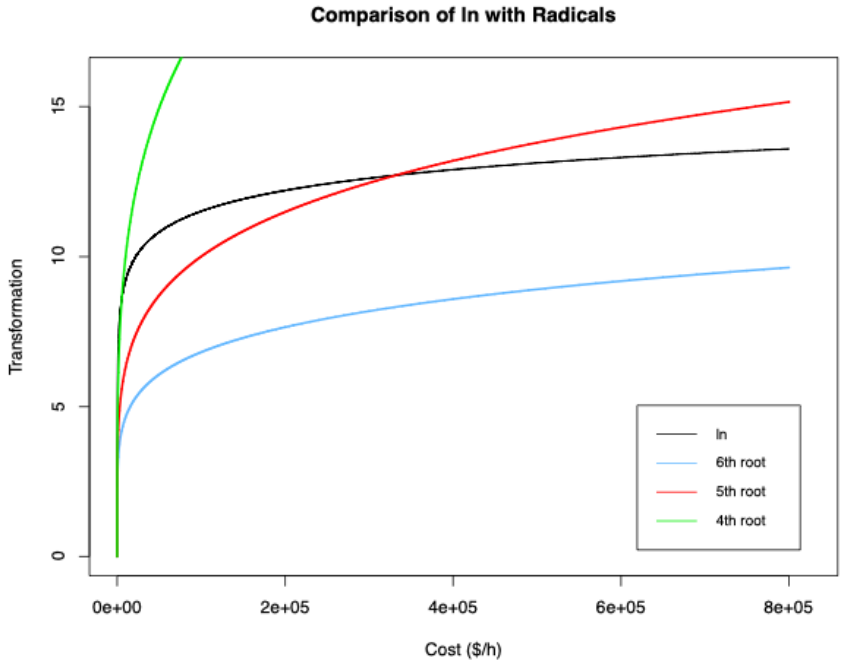

Figure 3. Comparison of ln with 4th, 5th, and 6th root radicals

The following are the revised versions of equations 1 and 2:

$$s = \frac{\ln h}{c^{1/5} \cdot \ln n}, \quad c > 0 \qquad (3)$$

$$s = \frac{\ln h}{|c-r|^{\frac{c-r}{5 \cdot |c-r|}} \cdot \ln n}, \quad |c-r| > 0 \qquad (4)$$

Table 3 depicts the five-number summary, plus the mean, for the susceptibility test with natural logarithm applied for both the cost-only and cost-reward models. We notice that both models show a more comparable scale than the previous two models while being right-skewed since the mean is higher than the median – the cost-reward model being less skewed as its mean is much closer to the median. Also, although still right-skewed, now the right skewness decreased noticeably for both models as the mean now lies within the middle 50 percent of the data. Furthermore, the range in the cost-reward is far less than that of the cost-only model.

Table 3. Summary statistics of *s* with natural logarithms

Min	Q1	Median	Mean	Q3	Max
0.055[a]	0.2875[a]	0.7101[a]	1.6326[a]	1.6805[a]	19.326[a]
0.058[b]	0.2911[b]	0.6821[b]	0.9029[b]	1.3031[b]	2.752[b]

[a] S Cost-Only Model
[b] S Cost-Reward Model

To further analyze them, a boxplot and histogram have been plotted for each of these logarithmic models in Figure 4.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

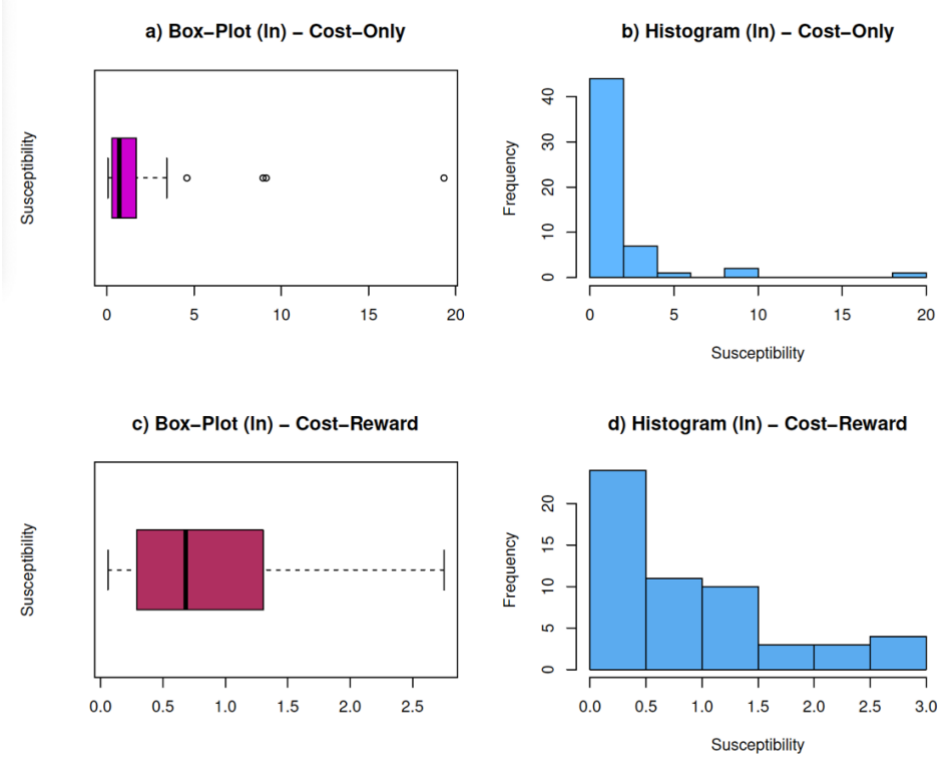

Figure 4. Histograms and boxplots for the logarithmic cost-only and cost-reward models

The boxplot in Figure 4.a shows that the outliers have significantly decreased from 10 to 4 outliers in the logarithmic cost-only model. In contrast, the boxplot in Figure 4.c suggests that the logarithmic cost-reward model seems to perfectly explain the data with no outliers. While still right-skewed, the histograms in Figure 4.b and 4.d, to some extent, show that the logarithmic models have a better distribution structure than their counterparts. This is particularly true for the logarithmic cost-reward model which closely resembles the right half of a bell-shaped normal distribution as depicted in Figure 4.d.

Table 4 portrays the logarithmic susceptibility values for both the cost-only and cost-reward models of the same cryptocurrency selection used in Table 1. The first 3 least susceptible cryptocurrencies remain the same as with the previous models. However, now in the new models the cryptos Hush and Litecoin Cash (LCC) are ranking better among the other cryptos than in the old models. It is observed that equations 3 and 4 give more weight to small differences in c, and $|c - r|$, than in equations 1 and 2. Therefore, the higher costs in Hush and Litecoin Cash respectively, though negligible (they are of the magnitude of less than 2 dollars), resulted in strengthening the network hashrate and reducing the susceptibility values. However, with the total rent hashrate in both Hush and LCC being greater than the network hashrate, the susceptibility value is still greater than one.

Moreover, we notice from the data that in general when the total rent hashrate and network hashrate are large in size, logarithmic differences between them tend to get less impacting which is due to the fact that at higher numbers the rate of change of logarithms get slower. Therefore, differences between total rent hashrates and network hashrates will manifest more in smaller scale cryptos than in larger scale ones. Similar to Table 1, Table 4 also shows that the s values in the cost-only and cost-reward models move together in the same direction with almost similar results, albeit the latter having slightly higher values. An exception was Veil where, against the expectations, the cost-reward model produced an s value less than 1. A closer examination of the whole list reveals that this case is repeated also for ZClassic and Arion. With the very large difference between the total rent hashrate and the network hashrate one would expect it to be very vulnerable.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 4. Calculated logarithmic *s* values for the same selection of the sample as in Table 1

Crypto	Code	Total Rent Hash H/s[a]	Net Hash H/s[a]	Cost $/h[b]	*S* Cost-Only	*S* Cost-Reward
Bitcoin	BTC	1.47800e+17	4.37695e+20	765434.3	0.05536638	0.05819616
Beam	BEAM	1.86400e+05	2.88500e+05	45.91243	0.44901109	0.45153561
Bitcoin Z	BTCZ	6.18600e+05	9.82300e+04	6.862904	0.78919968	0.80387556
.						
.						
.						
Hush	HUSH	9.92800e+08	1.04100e+07	2.353372	1.08037259	1.08889904
Litecoin Cash	LCC	1.47800e+17	4.29600e+14	0.7512779	1.24241490	1.27437320
Verge	XVG	1.50000e+12	9.78000e+12	0.1628868	1.34744247	1.36735274
Gemlink	GLINK	6.18600e+05	1.50700e+04	1.052876	1.37191968	1.39316739
BitTubeCash	TUBE	5.43123e+04	4.74000e+02	0.3773113	2.15040638	2.15898406
Veil	VEIL	1.47800e+17	3.90000e+09	0.00000682	19.32569181	0.92328884

[a] H/s = Hashes per second
[b] $/h = Cost of 1 hour attack in dollars

Coupled with slow rate of change at higher values in logarithms, the result in the cost-reward model for these cryptos was, also, due to the very low $|c - r|$ value which was less than 0.01 causing the numerator or denominator to be understated. This means that the cost-reward model penalizes very low rewards (or very low costs) and as such give a lower *s* value (or higher *s* value respectively).

Lastly, the model's efficacy and validity can be further substantiated by applying it on a selection of cryptocurrencies from outside the sample. Table 5 shows the results. Specifically, we observe that cryptocurrencies with network hashrates significantly surpassing the available rental hashrates for their PoW algorithms exhibit low *s* values, consistent with prior discussions. This pattern holds true for Monacoin, Ethereum Classic, and Dash. Additionally, the cost associated with launching a one-hour attack on these cryptocurrencies exceeds the potential rewards that can be obtained.

Table 5. Calculated logarithmic *s* value for cryptocurrencies from outside the sample

Crypto	Code	TRH H/s[a]	NH H/s[b]	Cost $/h[c]	BReward $[d]	$s_{cost\text{-}reward}$
Monacoin	MONA	6.7000e+09	6.6130e+13	1.189513e+02	5.13375000	0.2758148
Eth Classic	ETC	2.6983e+12	1.1998e+14	7.023360e+03	44.83840000	0.1503769
Dash	DASH	2.2820e+14	4.0100e+15	7.633844e+02	50.25791700	0.2473193
Trezarcoin	TZC	6.7130e+08	5.8700e+07	6.625523e-02	0.00811000	2.0070645
Aion	AION	9.9280e+08	5.1490e+04	1.164026e-02	0.00312615	4.9531723

[a] Total Rent Hashrate in Hashes per second
[b] Net Hashrate in Hashes per second
[c] Cost of 1 hour attack in dollars
[d] Block Reward in dollars

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Conversely, Trezarcoin and Aion demonstrate inadequate network hashrates when compared to the total rent hashrate available, and the costs are relatively negligible. Remarkably, the logarithmic cost-reward model, effectively elucidates this data, indicating higher *s* values. Hence, the model's ability to accurately explain these phenomena reinforces its robustness for analyzing the relationship between total rent hashrates, network hashrates, attack costs, block rewards, and susceptibility in cryptocurrencies.

4.2 Benchmarking the Susceptibility Test

We seek to find the threshold that distinguishes the degrees of resilience in PoW cryptocurrencies. In order to group these cryptocurrencies based on susceptibility, we need a criterion which is achieved by employing clustering analysis on the sample, specifically utilizing the k-means clustering method as explained in the methodology. This approach offers the advantage of segregating the cryptocurrencies in the sample into distinct clusters. Each cryptocurrency is assigned to a cluster based on its proximity to the centroid of that cluster.

Figure 5 depicts a plot of the k-means clustering performed on the susceptibility test of the cryptocurrency sample. Notably, the plot reveals a clear distinction among the five clusters formed. The plotted lines exhibit well-defined boundaries between the differently-shaped data points, indicating that observations within the same cluster are more similar to each other than to those in other clusters.

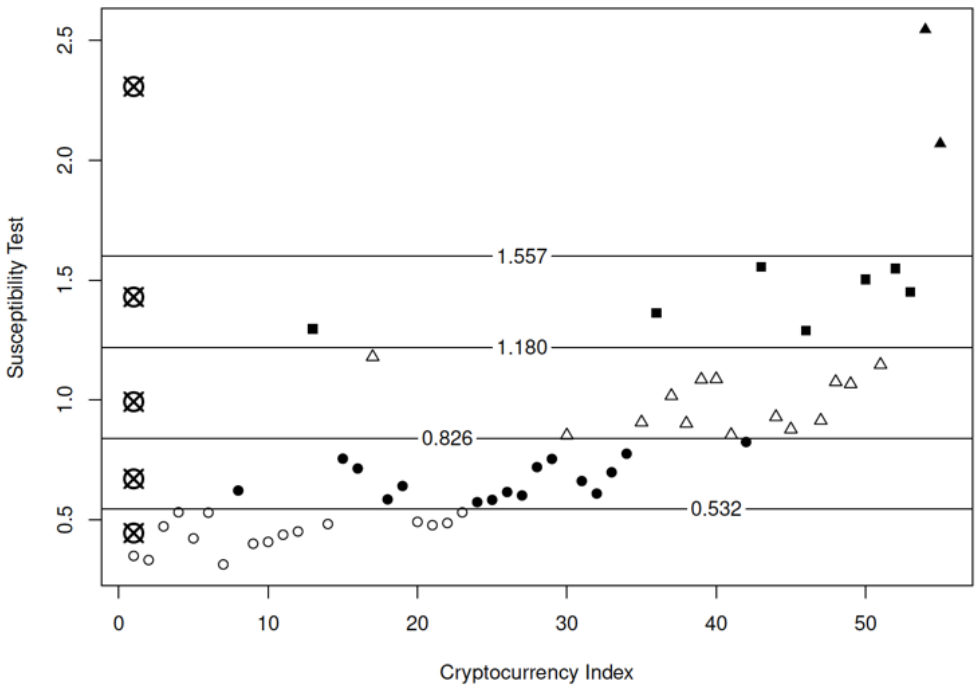

Figure 5. k-means clustering plot

It is important to note that the overall exponential pattern displayed by all the points holds no significant meaning in this context, as the susceptibility test clustering has been plotted against the cryptocurrency index. The pattern is a result of how the cryptocurrencies were sorted within the dataset.

The crossed circles on the plot represent the centroids of the clusters. These centroid positions reflect the average or central values of the data points within each cluster. The cluster consisting of open circle points exhibits a cluster center value of 0.445, with the susceptibility test having an upper bound value of 0.532. The cluster comprising black circle points has a cluster center value of 0.671, and the susceptibility test ranges from 0.532 to 0.826. The cluster containing open triangle points has a cluster center value of 0.993, with the susceptibility test ranging from 0.826 to 1.180. The cluster consisting of black square points has a cluster center value of 1.430, with the susceptibility test ranging from 1.180 to 1.557.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Lastly, the cluster comprising black triangle points has a cluster center value of 2.308, and the susceptibility test's lower bound is 1.557. These ranges indicate that the data points are densely grouped around their respective cluster centers, implying a high level of similarity within each cluster.

However, further insights can be drawn from clustering evaluation metrics which can explain the quality of the clustering results, indicating the degree of separation and coherence. These metrics are depicted in Table 6. The Dunn Index value of 1.844646 suggests that there is a moderate level of separation and compactness among the clusters. It indicates that there is some degree of distinction between the clusters, but the clusters may exhibit some overlap or lack optimal separation. In contrast, Calinski-Harabasz Index value of 385.8732 indicates a relatively high ratio, suggesting well-defined and compact clusters.

Table 6. Clustering Validation Indices

Indices			Scores
Dunn	Calinski–Harabasz	Davies–Bouldin	Silhouette
1.844646	385.8732	0.6074	0.6246461

This suggests that the clusters exhibit distinct patterns and are relatively homogeneous within themselves which is what we have intuitively deduced from looking at the plot. This finding suggests that the clustering algorithm was successful in creating distinct clusters with minimal overlap, highlighting its efficacy in capturing inherent patterns or structures in the data. The Davies-Bouldin Index resulted in a low value of 0.6074, which indicates that the clusters are indeed dissimilar. Silhouette Score, an assessment of individual data point assignments to clusters, yielded a mean score of 0.6246461. The reasonably high Silhouette Score suggests that the clustering algorithm achieved a notable level of cohesion and consistency in assigning data points to appropriate clusters.

Although the Dunn Index is relatively low, the minimum intercluster distance is still larger than the maximum intracluster distance because the value is greater than one. This calls for further research to study the existence of any potential overlap or suboptimal separation of clusters, despite the relatively high Calinski-Harabasz Index and high Silhouette Score. However, with the latter and coupled with a low Davies-Bouldin Index, it appears that the clustering results exhibit some level of separation and distinctiveness among the clusters, with a relatively high ratio of between-cluster dispersion to within-cluster dispersion and cluster dissimilarity.

Based on the clustering analysis above, the susceptibility test results have provided valuable insights into the security levels of cryptocurrencies. The open circle data points cluster, characterized by a cluster center of 0.445, showcases cryptocurrencies that exhibit a remarkable level of resilience against attacks, with susceptibility test values consistently below the critical threshold of 0.532. These cryptocurrencies can be considered as the epitome of robustness and security within the dataset. Conversely, the black triangle data points cluster, with a cluster center of 2.308, represents cryptocurrencies that display an alarming vulnerability to attacks, as their susceptibility test values surpass the threshold of 1.557.

Within the remaining clusters, we observe nuanced variations in security levels. The black circle data points cluster, centered at 0.671, encompasses cryptocurrencies with susceptibility test values ranging between 0.532 and 0.826. While these cryptocurrencies demonstrate a relatively lower vulnerability compared to the overall dataset, they still require continuous monitoring and appropriate security measures to maintain their current moderate level of resilience.

The open triangle data points cluster, centered at 0.993, comprises cryptocurrencies with susceptibility test values spanning from 0.826 to 1.180. This cluster represents a moderate level of vulnerability and lack of resilience. Lastly, the black square data points cluster, centered at 1.430, captures cryptocurrencies with susceptibility test values ranging between 1.180 and 1.557. This cluster signifies a high level of vulnerability.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

5. CONCLUSION

This study has focused on the critical 51% attack within the realm of PoW-based cryptocurrencies. Through an extensive literature review, it was evident that the existing research has remained silent about distinguishing the degrees of cryptocurrency resilience. The proposed approach aimed to fill this gap by developing a mathematical model, validated with observed data, to establish a robust susceptibility test formula.

The developed model provides a robust framework for assessing the vulnerability of cryptocurrencies to majority attacks. This approach moves beyond simplistic wait periods or market cap scales, which fail to capture the intricate dynamics of security and susceptibility in this context. Furthermore, the utilization of k-means clustering has facilitated the identification of benchmarking thresholds, enabling a more refined categorization of cryptocurrencies based on their susceptibility levels. The clustering analysis revealed distinct clusters, each representing a unique security profile within the dataset. The open circle data points cluster emerged as a beacon of resilience, showcasing cryptocurrencies with susceptibility test values consistently below the critical threshold of 0.532. Conversely, the black triangle data points cluster highlighted the alarming vulnerability of certain cryptocurrencies.

The benchmarks devised in this study contribute to the academic discourse on assessing the security of cryptocurrencies and perhaps gives a perspective on mitigating the risks associated with potential attacks. The findings provide researchers, industry practitioners, and policymakers with a solid foundation for identifying highly vulnerable cryptocurrencies and implementing appropriate security measures to safeguard against malicious activities. In contrast, the findings also provide the means for investors to manage the risk profiles of their investments and make more well-informed decisions.

As in any developed model, though, this study incorporates simplifications and assumptions to make the analysis tractable. Therefore, the outcomes from using the model should be regarded as informative indicators rather than definitive conclusions. A sugggestion that this research makes is to establish a third party organization that can use this model to provide indications about crypto investments or policy decisions, much like Fitch Ratings and Moodys do for ranking bank credit. Additionally, the model's effectiveness may diminish overtime should it not get updated periodically with latest data due to evolving crypto technologies. The interdisciplinary nature of this study, incorporating mathematical modeling, clustering analysis, and validation techniques, sets the ground for future research and the way forward.

Author Contributions Bekiroğlu A. M. designed the study, wrote the main manuscript text, and prepared all the figures.

Funding The author declares that no funds, grants, or other support were received during the preparation of this manuscript.

Data Availability The dataset supporting the conclusions of this article is available in Mendeley Data repository, with the name 'PoW Crypto Hashrates'reserved at DOI: 10.17632/wf7s8xy7wb.1.

DECLARATIONS

Competing Interest The author has no competing interests to declare that are relevant to the content of this article.

REFERENCES

[1] Aponte-Novoa, F. A., Orozco, A. L. S., Villanueva-Polanco, R., & Wightman, P. (2021). The 51% Attack on Blockchains: A Mining Behavior Study. IEEE Access, 9, 140549–140564. https://doi.org/10.1109/ACCESS.2021.3119291

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

[2] ATO. (2023). Crypto Asset Transactions. Australian Taxation Office. https://www.ato.gov.au/individuals/investments-and-assets/crypto-asset-investments/transactions---acquiring-and-disposing-of-crypto-assets/crypto-asset-transactions/

[3] Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015). SoK: Research perspectives and challenges for bitcoin and cryptocurrencies. 2015 IEEE Symposium on Security and Privacy, 2015-July, 104–121. https://doi.org/10.1109/SP.2015.14

[4] Browne, R. (2022). Central African Republic Becomes Second Country to Adopt Bitcoin as Legal Tender. CNBC. https://www.cnbc.com/2022/04/28/central-african-republic-adopts-bitcoin-as-legal-tender.html

[5] CoinMarketCap. (2023). All Cryptocurrencies. https://coinmarketcap.com/all/views/all/

[6] Conti, M., Kumar, E. S., Lal, C., & Ruj, S. (2018). A Survey on Security and Privacy Issues of Blockchain Technology. IEEE Communications Surveys & Tutorials, 20(4), 3416–3452. https://doi.org/10.1109/COMST.2018.2842460

[7] Courtois, N. T. (2014). On The Longest Chain Rule and Programmed Self-Destruction of Crypto Currencies. https://doi.org/10.48550/arXiv.1405.0534

[8] CRA. (2023). Guide for Cryptocurrency Users and Tax Professionals. Canada Revenue Agency. https://www.canada.ca/en/revenue-agency/programs/about-canada-revenue-agency-cra/compliance/digital-currency/cryptocurrency-guide.html

[9] DCI. (2020). 51% Attacks. MIT Media Lab Digital Currency Initiative. https://dci.mit.edu/51-attacks

[10] Dey, S. (2018). Securing Majority-Attack in Blockchain Using Machine Learning and Algorithmic Game Theory: A Proof of Work. 2018 10th Computer Science and Electronic Engineering Conference, CEEC 2018 - Proceedings, 7–10. https://doi.org/10.1109/CEEC.2018.8674185

[11] Duong, T., Fan, L., Katz, J., Thai, P., & Zhou, H.-S. (2020). 2-hop Blockchain: Combining Proof-of-Work and Proof-of-Stake Securely. In L. Chen, N. Li, K. Liang, & S. Schneider (Eds.), Computer Security – ESORICS 2020 (Vol. 12309, pp. 697–712). Springer, Cham. https://doi.org/10.1007/978-3-030-59013-0_34

[12] Dusart, V. (2023). Proof-of-stake (PoS). Ethereum.Org. https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/

[13] FinCEN. (2013). Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies.

[14] Guo, H., & Yu, X. (2022). A survey on blockchain technology and its security. Blockchain: Research and Applications, 3(2), 100067. https://doi.org/10.1016/j.bcra.2022.100067

[15] Hasanova, H., Baek, U., Shin, M., Cho, K., & Kim, M.-S. (2019). A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. International Journal of Network Management, 29(2). https://doi.org/10.1002/nem.2060

[16] IRS. (2014). Notice 2014-21.

[17] König, L., Unger, S., Kieseberg, P., & Tjoa, S. (2020). The Risks of the Blockchain A Review on Current Vulnerabilities and Attacks. Journal of Internet Services and Information Security, 10(3), 110–127. https://doi.org/10.22667/JISIS.2020.08.31.110

[18] Lansky, J. (2020). Cryptocurrency Survival Analysis. Journal of Alternative Investments, 22(3), 55–64. https://doi.org/10.3905/jai.2019.1.084

[19] Larson, R., & Farber, B. (2019). Elementary Statistics: PICTURING THE WORLD (7th ed.). Pearson Education Limited.

[20] Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on the security of blockchain systems. Future Generation Computer Systems, 107, 841–853. https://doi.org/10.1016/j.future.2017.08.020

[21] Maghdeed, F. (2020a). The Transformation of the Traditional Equity Market to a Blockchain Securitized Asset Market. Medium.Com. https://medium.com/@farhang.maghdeed/the-transformation-of-the-traditional-equity-market-to-a-blockchain-securitized-asset-market-dfab0b4c96ff

[22] Maghdeed, F. (2020b). From Digital Currency to Cryptocurrency: What are the main differences between them. Medium.Com. https://medium.com/@farhang.maghdeed/from-digital-currency-to-cryptocurrency-what-are-the-main-differences-between-them-cf16439526f3

[23] Mrazek, K., Holton, B., Cathcart, C., Speirer, J., Do, J., & Mohd, T. K. (2022). Risks in Blockchain - A Survey about Recent Attacks with Mitigation Methods and Solutions for Overall. 2022 IEEE International Conference on Electro Information Technology (EIT), 5–10. https://doi.org/10.1109/eIT53891.2022.9813975

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

[24] Nguyen, C. T., Hoang, D. T., Nguyen, D. N., Niyato, D., Nguyen, H. T., & Dutkiewicz, E. (2019). Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities. IEEE Access, 7, 85727–85745. https://doi.org/10.1109/ACCESS.2019.2925010

[25] NiceHash. (2023). Hashpower Marketplace. NiceHash.Com. https://www.nicehash.com/my/marketplace/SHA256ASICBOOST

[26] Niranjani, V., Sanjaay Kamachi, P. S., Siddhaarth, S., Venkatachalam, B., & Vishal, N. (2022). Hybrid approach to minimize 51% attack in Cryptocurrencies. 2022 8th International Conference on Advanced Computing and Communication Systems, ICACCS, 2100–2103. https://doi.org/10.1109/ICACCS54159.2022.9785161

[27] Novet, J. (2022). Tesla has dumped 75% of its bitcoin holdings a year after touting "long-term potential." CNBC. https://www.cnbc.com/2022/07/20/tesla-converted-75percent-of-bitcoin-purchases-to-fiat-currency-in-q2-2022.html

[28] Omardonia. (2023). How to Choose the Right Clustering Algorithm for Your Data. Generative AI. https://generativeai.pub/how-to-choose-the-right-clustering-algorithm-for-your-data-8f3ee24b9c16

[29] Ozturk, F. E. (2023). Unsupervised Learning in R: Determination of Cluster Number. Medium.Com. https://medium.com/@ozturkfemre/unsupervised-learning-determination-of-cluster-number-be8842cdb11

[30] Profit-mine. (2023). Coins. Profit-Mine.Com. https://profit-mine.com/en/coins

[31] Quarteroni, A. (2009). Mathematical models in science and engineering. Notices of the American Mathematical Society, 56(1), 10–19.

[32] Ramos, S., Pianese, F., Leach, T., & Oliveras, E. (2021). A great disturbance in the crypto: Understanding cryptocurrency returns under attacks. Blockchain: Research and Applications, 2(3), 100021. https://doi.org/10.1016/j.bcra.2021.100021

[33] Rodriguez, M. Z., Comin, C. H., Casanova, D., Bruno, O. M., Amancio, D. R., Costa, L. da F., & Rodrigues, F. A. (2019). Clustering algorithms: A comparative approach. PLoS ONE, 14(1), 1–34. https://doi.org/10.1371/journal.pone.0210236

[34] Sayeed, S., & Marco-Gisbert, H. (2019). Assessing Blockchain Consensus and Security Mechanisms Against the 51% Attack. Applied Sciences, 9(9). https://doi.org/10.3390/app9091788

[35] Scicchitano, F., Liguori, A., Guarascio, M., Ritacco, E., & Manco, G. (2020). A Deep Learning Approach for Detecting Security Attacks on Blockchain. CEUR Workshop Proceedings, 2597, 212–222.

[36] Shanaev, S., Shuraeva, A., Vasenin, M., & Kuznetsov, M. (2020). Cryptocurrency Value and 51% Attacks: Evidence from Event Studies. Journal of Alternative Investments, 22(3), 65–77. https://doi.org/10.3905/jai.2019.1.081

[37] Wen, X., Chen, Y., Zhang, W., Jiang, Z. L., & Fang, J. (2022). Blockchain Consensus Mechanism Based on Quantum Teleportation. Mathematics, 10(14), 1–9. https://doi.org/10.3390/math10142385

[38] WhatToMine. (2023). Crypto Coins Mining Profit Calculators. WhatToMine.Com. https://whattomine.com/calculators

[39] Yang, X., Chen, Y., & Chen, X. (2019). Effective scheme against 51% Attack on Proof-of-Work Blockchain with History Weighted Information. 2019 IEEE International Conference on Blockchain (Blockchain), 261–265. https://doi.org/10.1109/Blockchain.2019.00041

[40] Zhang, Y., Yang, W., Chen, W., & Xue, L. (2022). Short Sale Attack: A PoW-blockchain-aimed attacking model via short sale. 2022 IEEE International Conference on Electrical Engineering, Big Data and Algorithms (EEBDA), 1240–1246. https://doi.org/10.1109/EEBDA53927.2022.9744958

[41] Zhao, J. L., Fan, S., & Yan, J. (2016). Overview of business innovations and research opportunities in blockchain and introduction to the special issue. Financial Innovation, 1(28), 1–7. https://doi.org/10.1186/s40854-016-0049-2

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.