The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM)
ISSN: 2602-3199

The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM), 2023

Volume 23, Pages 202-208

ICRETS 2023: International Conference on Research in Engineering, Technology and Science

Blockchain Security-Efficiency Analysis based on DEA-SBM Model

Thi Minh Nhut Vo
National Kaohsiung University of Science and Technology

Chia-Nan Wang
National Kaohsiung University of Science and Technology

Fu-Chiang Yang
National Kaohsiung University of Science and Technology

Van Thanh Tien Nguyen
Industrial University of Ho Chi Minh City

Abstract: It is estimated that by 2023 the security market will reach a value of $1.4 billion. This growth is primarily driven by the increasing use of technology in sectors like finance, healthcare and logistics. As more companies adopt technology there is a growing need to protect their data from hacking and other malicious activities. The security of the network plays a role in ensuring the implementation and adoption of technology. Given the rise in cyberattacks and data breaches it is expected that the importance of security will continue to grow in the coming years. In this study we will explore some companies that specialize in providing security solutions. Our analysis will be based on three factors and two desired outcomes. The selected companies include Hacken, Quantstamp, OpenZeppelin, Trail of Bits, ConsenSys, Certik, LeastAuthority, PWC Switzerland, Slowmist and Runtime Verification. The purpose of this research paper is to assess the effectiveness of the security industry for decision makers, experts and government entities. By gaining insights into this sector and enhancing network security measures for implementations, across industries.

Keywords: Blockchain security, Efficiency analysis, DEA-SBM model, Cybersecurity companies, Network security.

Introduction

The market, for technology has seen growth in recent years and is projected to reach a value of $1.4 billion by 2023. The widespread adoption of technology across industries like finance, healthcare and logistics has contributed to its rising popularity. However companies involved in blockchain face challenges in safeguarding their data against hacking and other criminal activities.

In this study, our focus lies on examining the ten firms in the market for their expertise in ensuring secure blockchain systems. These firms include Hacken, Quantstamp, OpenZeppelin, Trail of Bits, ConsenSys, Certik, LeastAuthority, PWC Switzerland, Slowmist and Runtime Verification. Through our research findings we aim to guide policymakers, experts and governments in enhancing security measures within the network.

To determine the firms within the blockchain security landscape our selection criteria consider factors such as market capitalization revenue generation and reputation through analyzing variables like employee count R&D expenditure and marketing costs as input metrics and revenue generation, profitability and market share, as output metrics we assess these companies effectiveness.

The DEA SBM approach is used to assess the effectiveness of companies operating in the security sector. Through data analysis we gain insights, into the performance of the security industry highlighting both businesses and areas that require improvement. This information can be invaluable for decision makers, professionals and governments when making investment decisions implementing regulations and providing industry support. Furthermore by deepening our understanding of the security challenges faced by companies this research contributes to the adoption and implementation of technology across various industries. We strive to enhance network security and integrity within the blockchain ecosystem. The study identifies performing businesses in this field while employing DEA SBM techniques to evaluate their effectiveness. The findings from our research will drive industry growth. Facilitate utilization of blockchain technology, across multiple sectors.

Literature Review

Creating access control policies that can be customized to a degree along, with implementing a mechanism to prevent tampering or violation of rules, within the IoT platform will undoubtedly play a crucial role in the widespread adoption of IoT based solutions. A. Rizzardi et. AL. suggest incorporating a permissioned blockchain into a distributed middleware layer that's honest but not trusted (Rizzardi et al., 2022). The goal is to ensure resource access management, for all parties. In their study, Li et. Al. (2022) suggest an approach called PDGNN (Phishing Detection Graph Neural Network) to counteract phishing attacks. However the computational demands and storage needs associated with this framework also present an obstacle when it comes to spreading messages (Li, Xie, Xu, Zhou, & Xuan, 2022) . Vishwakarma et. al. (2022) have proposed the introduction of a security protocol called LBSV. This lightweight blockchain based solution aims to address the challenges related to secure communication and storage in the context of SDN enabled IoV (Vishwakarma, Nahar, & Das, 2022). In their study (Zur et. Al., 2022) researchers proposed a model that incorporates transaction fees as variable block rewards making it more realistic (Bar-Zur, Abu-Hanna, Eyal, & Tamar, 2022). They introduced "Proof of Work" (PoUW) based on the concept of Proof of Work (PoW) where the resources wasted in PoW are utilized for calculations. Another interesting approach called "Proof of Learning" (PoLe) was suggested by (Zhang et. al., 2022) which utilizes the wasted resources to train machine learning models (B. Zhang, Zhang, & Sun, 2022). With the advancements, in intelligence we now have automated tools that leverage learning and machine learning algorithms to make predictions about cancer. Nasir et. Al. Conducted a study where they introduced a model that combines the Internet of Medical Things (IoMT) transfer learning techniques and deep learning algorithms to identify early stage kidney cancer (Nasir et al., 2022). To ensure the security of patients data this model incorporates clouds based on technology and transfer learning trained models. In their study, Aljumaie et. al., 2022 propose a version of the LEACH PRO protocol that incorporates security techniques to safeguard Wireless Sensor Networks (WSNs) (Aljumaie & Alhakami, 2022).

Zhao et. al., 2022 conducted a study that combines the efficiency slack based measure (SBM) model and the window analysis model to assess the CEE (customer experience excellence) in the freight transport industry across 31 Chinese provinces from 2008, to 2019 (Zhao et al., 2022). Meanwhile Zhang et. al., 2022 aimed to understand the factors influencing residents participation in sports consumption and provide insights, for enterprises to develop marketing strategies. They developed an integrated framework that focuses on participation sports service products and takes into account the preferences and demands of participation sports consumers (T. Zhang, Wang, & neuroscience, 2022). In Huangs study conducted in 2022 a model based on factor analysis was employed to assess and rank the sports abilities of provinces, in China (Huang, 2022). This industry faces a challenge due, to the scarcity of workers to fill roles, which negatively impacts its potential for sustainable growth. Therefore the researchers chose a approach to examine the textual data provided by experts.

Methodology

The Research Frameworks

Selection of the Ten Most Successful Blockchain Security Companies

The process of selecting companies in the security industry involved considering important factors to ensure a well rounded and diverse representation of successful players, in the field. These factors included both quantitative aspects with the goal of identifying companies that have demonstrated their expertise built a reputation, in the market and have a history of innovation (C.-N. Wang, Yang, Vo, & Nguyen, 2023; C. N. Wang, Yang, Vo, & Nguyen, 2022).

In Table 1 you will find a list of Decision Making Units (DMUs) that consist of organizations operating in the blockchain security market. Each DMU is identified by a code. Accompanied by the name of the corresponding firm. The table encompasses companies, each, with its distinct role and impact, on the field of blockchain security.

Table 1. List of DMUs

DMU	Company Name
B1	Hacken
B2	Quantstamp
B3	OpenZeppelin
B4	Trail of Bits
B5	ConsenSys
B6	Certik
B7	LeastAuthority
B8	PWC Switzerland
B9	Slowmist
B10	Runtime Verification

Selection of Input and Output Variables

When evaluating companies, in the security industry it is crucial to select the input and output variables. These variables help us understand how efficient and successful these companies are. We have chosen variables for this assessment;

Input Variables:

- **Investment in Research and Development (R&D)**: This reflects how much a company invests in innovation and technology development. Companies that allocate resources to R&D are likely to be focused on staying in blockchain security advancements and offering cutting edge solutions.
- **Employee Expertise:** The qualifications and expertise of a company's workforce play a role as an input variable. Skilled employees contribute to the company's efficiency and their ability to deliver top notch security services.
- **Security Partnerships**: Collaborations with organizations to enhance security capabilities demonstrate a company's efforts to leverage expertise and resources. Strategic partnerships can lead to improved efficiency and a wider range of security solutions.

Output Variables:

- **Market Share**: This refers to the portion of the market that a company has been able to capture. On the hand Customer Satisfaction is an indicator that measures the level of satisfaction among clients or customers.
- **Customer Satisfaction**: A company's competitiveness and ability to attract and retain clients can be gauged by its market share.

When it comes to measuring the level of satisfaction clients experience with a companys services customer satisfaction becomes a factor. High customer satisfaction indicates that the company meets client expectations delivers value and fosters customer loyalty and repeat business. The choice of input and output variables, in evaluating efficiency in the blockchain security industry aligns with goals. Input variables such as R&D expenditure and employee expertise reflect the companys commitment to innovation and expertise. On the hand market share and customer satisfaction as output variables provide insights into the companys performance in the market and levels of client satisfaction.

Considering these variables collectively an efficiency analysis will comprehensively evaluate how selected companies utilize their resources and efforts to achieve outcomes in the blockchain security sector. The findings will help identify companies uncover practices and highlight areas, for potential improvement. Ultimately this will contribute to a innovative blockchain ecosystem.

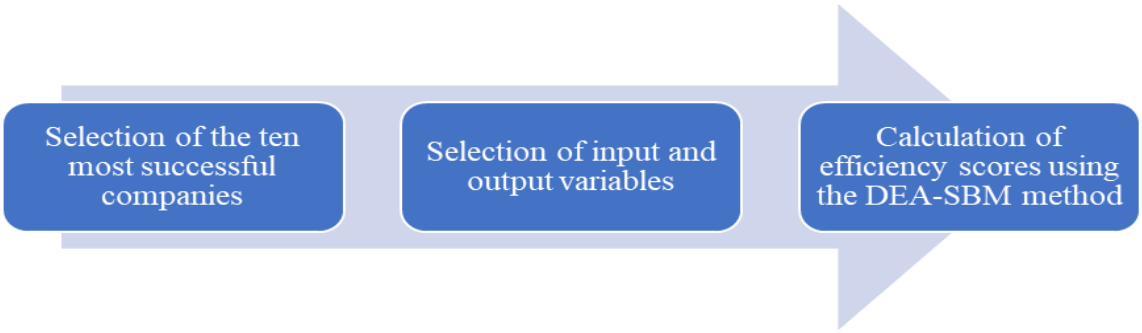


Figure 1. Calculation process of efficiency scores

Calculation of Efficiency Scores Using the DEA-SBM Method

In years the attention, towards technology has grown significantly due to its potential to enhance security across various industries. The initial step in evaluating security effectiveness involves identifying the 10 companies operating within this sector. Once these top 10 companies are determined the subsequent step entails selecting the input and output variables that will be used for analysis. The statistics in Table 2 provide insights into performance metrics. Serve as a basis for assessing and comparing the efficiency and effectiveness of the DMUs in terms of blockchain security. If theres a deviation it means there's more variability, among the DMUs regarding that specific variable. The Average column gives us an idea of what values we can expect to see across the DMUs helping us understand how they perform as a whole.

Table 2. Statistics on input/output data

	R&D Expenditure	Employee Expertise	Security Partnerships	Market Share	Customer Satisfaction
Max	9	9	9	9	9
Min	3	6	6	3	3
Average	7.4	8.1	7.5	6	7
SD	1.959591794	1.374773	1.5	2.569047	2.366432

Table 3. Correlation on input and output data.

	R&D Expenditure	Employee Expertise	Security Partnerships	Market Share	Customer Satisfaction
Research and Development (R&D) Expenditure	1	0.801784	0.51031	0.556187	0.603807
Employee Expertise	0.801783726	1	0.654654	0.764471	0.737711
Security Partnerships	0.510310363	0.654654	1	0.856349	0.676123
Market Share	0.55618651	0.764471	0.856349	1	0.789542
Customer Satisfaction	0.603807364	0.737711	0.676123	0.789542	1

When examining security efficiency potential input variables may include power, storage capacity, employee count and research and development expenditures. On the hand possible output variables could encompass metrics, like implementation of blockchain solutions instances of security breaches detected and cost savings experienced by consumers through utilizing blockchain technology (see Table 3).

The Average column gives us a perspective of the values we observe across the different DMUs. The findings reveal correlations between Research and Development (R&D) Expenditure and Employee Expertise (0.801) Security Partnerships (0.510) Market Share (0.556) as well, as Customer Satisfaction (0.604). By utilizing the DEA SBM model blockchain security companies can assess their efficiency and effectiveness compared to their peers. Moreover this approach helps identify areas for performance improvement by analyzing factors contributing to inefficiency or ineffectiveness.

Additionally the DEA SBM model serves as a benchmarking tool, for comparing security systems or companies. This analysis helps identify which companies are performing well. Armed with this information investors can make decisions, about where to invest their resources.

The SBM model evaluates a companys efficiency by measuring its slack resources that can be utilized for improvement. These slack resources represent potential that if properly leveraged can enhance a companys performance. Unlike the DEA model the SBM model provides a comprehensive and realistic assessment of performance by considering these untapped resources and their impact, on efficiency.

$$P = \{(x,y) | \, x \geq \sum_{j=1}^{n} \quad \beta_j x_j, 0 \leq y \leq \sum_{j=1}^{n} \quad \beta_j y_j, \beta \geq 0\} \quad (1)$$

$\beta_j = (\beta_1, \beta_2, \ldots, \beta_n)^T$ Is called the intensity vector

To change the inequalities in equation (1) to equalities, we can introduce slacks for the J as follows:

$$x = \sum_{j=1}^{n} \quad \beta_j x_j + s^-$$

$$y = \sum_{j=1}^{n} \quad \beta_j y_j - s^+$$

$$s^- \geq 0, s^+ \geq 0,$$

The slacks that are denoted as Where $s^- = (s^-_1, s^-_2, \ldots, s^-_m) \in R^m$ and $s^+ = (s^+_1, s^+_2, \ldots, s^+_m) \in R^S$ respectively are referred to as input and output slacks.

The SBM model is designed to tackle a programming problem. Its goal is to maximize the efficiency score (θ) while ensuring that the slack variables are non negative and the inputs and outputs of DMUs (Decision Making Units) are properly weighted. This approach provides an efficiency score, for each DMU indicating how effectively it utilizes its resources and produces outputs. To put it simply the SBM model is a tool for assessing the performance of DMUs across industries. By considering slack variables it offers a comprehensive evaluation of efficiency enabling us to pinpoint areas with potential for improvement.

Data Analysis and Discussion

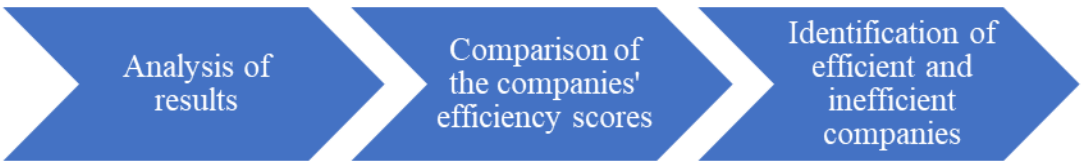
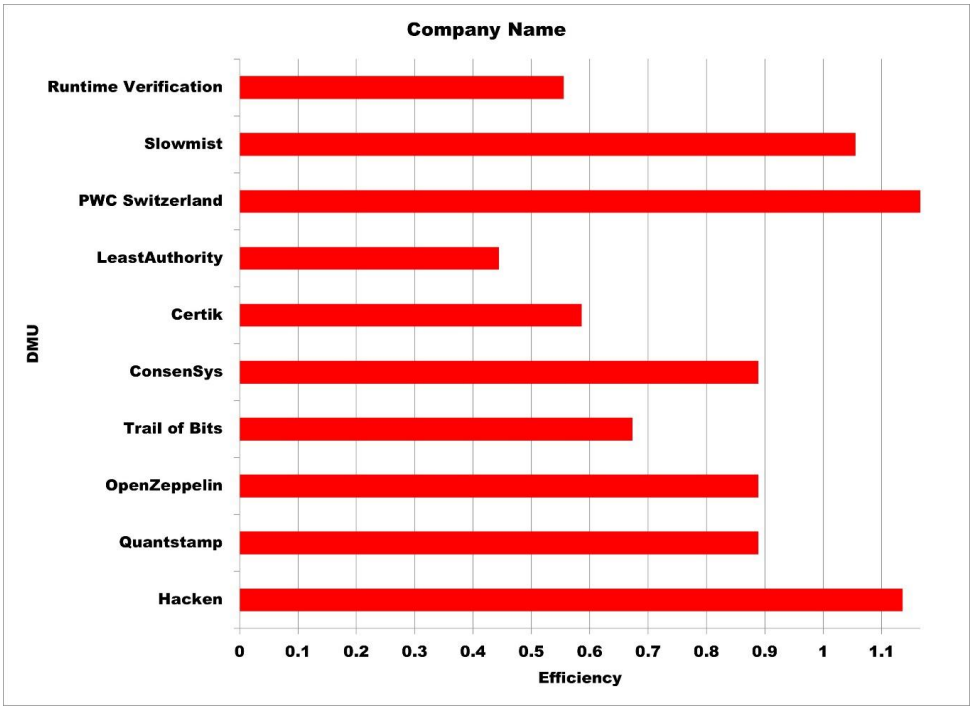


Figure 2. Data analysis process.

In figure 2, we can move forward with our analysis using DEA SBM approach involved calculating efficiency scores for each company under consideration. The outcomes revealed that certain companies were more effective than others, in utilizing resources to accomplish their objectives. Indeed the study revealed that PWC Switzerland and ConsenSys performed well in terms of efficiency whereas Slowmist and Certik showed levels of efficiency.

In Figure 3, you can see a list of the 10 blockchain security companies. This ranking is based on their performance metrics, which determine their positions. Each company has its position with the highest ranked company being recognized as the most effective and successful, in their blockchain security effortsWhen we compared the efficiency scores of companies we noticed differences, in how they utilized their input and output variables. For example PWC Switzerland scored well in terms of power while ConsenSys excelled in the number of implementations. On the hand both Slowmist and Certik received scores in both categories. Based on this analysis we can conclude that inefficient companies were identified based on their resource utilization. Companies with high efficiency scores showed allocation of resources to achieve their objectives. In contrast those with scores were considered ineffective, in utilizing their resources. As a result PWC Switzerland and ConsenSys emerged as companies while Slowmist and Certik were categorized as performers.

Figure 3. Ranking of 10 blockchain security companies



Conclusion

The DEA SBM method is an essential tool, for evaluating the efficiency of companies across industries. Its impact becomes more significant in the field of security. The studys The study reveals insights, into ten companies operating in this industry. Highlights the ability of the DEA SBM to identify the most efficient players based on their effective use of input and output variables. By differentiating between companies this research provides information for decision makers and investors showcasing the effectiveness of various blockchain security firms. In a changing security landscape maintaining efficiency and effectiveness is crucial. The DEA SBM model serves as a tool for companies in this industry guiding them towards success and innovation. It helps security firms refine their strategies and improve performance by identifying areas that need improvement. Moreover this model not benefits company operations. Also provides investors with well informed insights to channel investments towards the most promising and efficient players. Looking ahead future studies that utilize the DEA SBM approach will undoubtedly play a role in harnessing the potential of technology. As the emerging blockchain security industry continues to advance it is essential to understand and optimize its efficiency for adoption and transformative impact. Researchers and stakeholders can leverage the power of the DEA SBM model to unlock avenues of growth and innovation within this industry. In summary the DEA SBM model proves to be a methodology, for evaluating the efficiency and effectiveness of security systems and companies operating in this field. Its capacity to reveal discrepancies, in effectiveness and recognize chances for enhancement renders it a crucial tool for bolstering the performance and competitiveness of the security sector. Embracing this strategy is not optional; rather it is imperative for any participant seeking success, in the evolving domain of security.

Scientific Ethics Declaration

The authors declare that the scientific ethical and legal responsibility of this article published in EPSTEM journal belongs to the authors.

Acknowledgements or Notes

* This article was presented as an oral presentation at the International Conference on Research in Engineering, Technology and Science (www.icrets.net) held in Budapest/Hungary on July 06-09, 2023.

* The authors would like to thank the Ministry of Science and Technology, Taiwan. We also would like to thank the National Kaohsiung University of Science and Technology, Industrial University of Ho Chi Minh City, and Thu Dau Mot University for their assistance. Additionally, we would like to thank the reviewers and editors for their constructive comments and suggestions to improve our work.

References

Aljumaie, G. S., & Alhakami, W. J. S. (2022). A secure LEACH-PRO protocol based on blockchain. *Sensors, 22*(21), 8431.

Bar-Zur, R., Abu-Hanna, A., Eyal, I., & Tamar, A. (2022). WeRLman: to tackle whale (transactions), go deep (RL). *Proceedings of the 15th ACM International Conference on Systems and Storage, 148-148.*

Huang, Y. (2022). The role of artificial intelligence technology in promoting the development of my country's sports industry. *The 2nd International Conference on Artificial Intelligence, Automation, and High-Performance Computing (AIAHPC 2022).*

Li, P., Xie, Y., Xu, X., Zhou, J., & Xuan, Q. (2022). Phishing fraud detection on ethereum using graph neural network. *Proceedings International Conference on Blockchain and Trustworthy System, 362-375, Singapore: Springer Nature Singapore.*

Nasir, M. U., Zubair, M., Ghazal, T. M., Khan, M. F., Ahmad, M., Rahman, A.-u., . . . Mansoor, W. J. S. (2022). Kidney cancer prediction empowered with blockchain security using transfer learning. *Sensors*, 22(19), 7483.

Rizzardi, A., Sicari, S., Miorandi, D., & Coen-Porisini, A. (2022). Securing the access control policies to the Internet of Things resources through permissioned blockchain. *Concurrency and Computation: Practice and Experience, 34*(15), e6934..

Vishwakarma, L., Nahar, A., & Das, D. (2022). Lbsv: Lightweight blockchain security protocol for secure storage and communication in sdn-enabled iov. *IEEE Transactions on Vehicular Technology, 71*(6), 5983-5994.

Wang, C.-N., Yang, F.-C., Vo, N. T., & Nguyen, V. T. T. J. B. (2023). Enhancing Lithium-Ion battery manufacturing efficiency: A comparative analysis using DEA malmquist and epsilon-based measures. *Batteries*, *9*(6), 317.

Wang, C. N., Yang, F. C., Vo, N. T. M., & Nguyen, V. T. T. (2022). Wireless communications for data security: efficiency assessment of cybersecurity industry-A promising application for UAVs. *Drones*, *6*(11). https://doi.org/10.3390/drones6110363

Zhang, B., Zhang, B., & Sun, J. (2022, August). Pole-2p: Improved consensus algorithm based on proof of learning. In *Second International Conference on Digital Signal and Computer Communications (DSCC 2022) (Vol.* 12306, pp. 209-214). SPIE.

Zhang, T., & Wang, W. (2022). Consumer group identification algorithm for ice and snow sports. *Computational Intelligence and Neuroscience*, Article ID 2174910. https://doi.org/10.1155/2022/2174910

Zhao, X., Wang, J., Fu, X., Zheng, W., Li, X., & Gao, C. (2022). Spatial–temporal characteristics and regional differences of the freight transport industry's carbon emission efficiency in China. *Environmental Science and Pollution Research, 29*(50), 75851-75869.

Author Information

Thi Minh Nhut Vo
National Kaohsiung University of Science and Technology,
415 Jiangong, Sanmin, Kaohsiung, Taiwan
Thu Dau Mot University, Vietnam

Chia-Nan Wang
National Kaohsiung University of Science and Technology,
415 Jiangong, Sanmin, Kaohsiung, Taiwan

Fu-Chiang Yang
National Kaohsiung University of Science and Technology,
415 Jiangong, Sanmin, Kaohsiung, Taiwan

Van Thanh Tien Nguyen
Industrial University of Ho Chi Minh City
12, Nguyen Van Bao, Go Vap, Ho Chi Minh City, Vietnam
Corresponding author contact e-mail: *thanhtienck@ieee.org*

To cite this article:

Vo, T.M.N., Wang, C.N., Yang, F.C. & Nguyen, V.T.T. (2023). Blockchain security- efficiency analysis based on DEA-SBM Model. *The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM), 23*, 202-208.