User Transaction Patterns in Smart Contracts Based on Call Frequency and Transfer Value

Hery[1,*], Calandra Haryani[2]

[1,2]Department of Information Systems, Pelita Harapan University, Jalan M.H. Thamrin Boulevard No.1100 Lippo Karawaci, Tangerang, 15811, Indonesia

ABSTRACT

Smart contracts are integral to blockchain technology, enabling decentralized and automated transactions. This study examines 1,000 smart contracts by analyzing metrics such as total transactions, unique users, total value transferred (ETH), gas consumption, and call frequency. Total transactions range from 1 to 18,902, with unique users spanning 1 to 14,839. The average total value transferred is 3,245.87 ETH, peaking at 7,850.16 ETH, while gas consumption averages 25,486,392 units with a maximum of 58,471,065 units. Strong correlations were identified between transaction volume (r = 0.78), user engagement, and gas consumption. Clustering analysis categorizes contracts into low, moderate, and high-activity groups, while anomaly detection highlights 32 contracts with unusual behaviors, indicating inefficiencies or vulnerabilities. These findings emphasize the importance of optimizing smart contract designs to improve efficiency, security, and scalability. The study provides actionable insights into operational patterns and proposes future research directions, including design optimization, real-time monitoring, cross-platform analysis, and machine learning applications for predictive modeling. By addressing these aspects, this research contributes to the ongoing development of robust and efficient decentralized systems.

Keywords Smart Contracts, Blockchain Technology, Anomaly Detection, Clustering Analysis, Decentralized Systems Efficiency

INTRODUCTION

Blockchain technology has revolutionized the way digital transactions are conducted, offering decentralized, secure, and transparent systems [1]. Initially conceptualized as the underlying technology for Bitcoin, blockchain has since evolved into a versatile framework powering various applications across industries, including finance, supply chain management, healthcare, and gaming [2]. At the core of this innovation are smart contracts, self-executing protocols that facilitate and enforce agreements without intermediaries. By automating complex processes and reducing reliance on trust, smart contracts can enhance efficiency and reduce costs in a wide range of scenarios. Smart contracts operate on decentralized platforms, with Ethereum being one of the most prominent examples [3]. These contracts are coded with specific conditions and actions that execute automatically when predefined criteria are met. For instance, in financial transactions, a smart contract could release payment to a supplier once a shipment is confirmed, eliminating delays and minimizing errors [4]. This automation has led to widespread adoption, particularly in Decentralized Finance (DeFi) and Non-Fungible Token (NFT) ecosystems, where smart contracts handle billions of dollars in transactions daily. Despite their transformative potential, smart contracts present unique challenges. While advantageous, the transparency and immutability of blockchain also make errors and vulnerabilities in contract design particularly

Submitted: 7 April 2025
Accepted: 12 May 2025
Published: 23 August 2025

Corresponding author
Hery, hery.fik@uph.edu

Additional Information and Declarations can be found on page 244

DOI: 10.47738/ijrm.v2i3.35

costly [5]. Issues such as re-entrance attacks, gas inefficiencies, and unintended behaviors have highlighted the critical need for robust design, thorough testing, and ongoing monitoring. Moreover, as the adoption of smart contracts grows, understanding their operational characteristics becomes increasingly important to ensure scalability, security, and efficiency [6].

This study aims to address these challenges by analyzing the operational metrics of 1,000 smart contracts. By focusing on key attributes such as total transactions, unique users, total value transferred, gas consumption, and transfer call frequency, this research seeks to uncover patterns and relationships that can inform the design and optimization of smart contracts [7]. Through statistical analysis, clustering techniques, and anomaly detection, this study provides actionable insights into smart contracts' efficiency, security, and scalability, contributing to the broader understanding of decentralized systems and their practical applications across various sectors. The findings aim to support developers, researchers, and policymakers in creating more reliable and efficient blockchain ecosystems [8]. Blockchain technology has transformed the landscape of digital transactions by introducing decentralized, secure, and transparent systems. At the heart of this innovation lie smart contracts, self-executing protocols that facilitate and enforce agreements without intermediaries. These contracts have revolutionized industries ranging from finance and supply chain management to gaming and healthcare by automating complex processes while ensuring trust and efficiency.

Despite their growing adoption, understanding the operational characteristics of smart contracts remains a critical area of research. Factors such as transaction volume, user engagement, and resource consumption can significantly influence the performance and scalability of these systems. Furthermore, the inherent transparency of blockchain networks presents opportunities to analyze and optimize smart contract behavior, revealing insights into their efficiency, security, and potential vulnerabilities. This study aims to provide a comprehensive analysis of 1,000 smart contracts, focusing on key metrics that define their operation. By examining total transactions, unique users, total value transferred, gas consumption, and transfer call frequency, this research seeks to uncover patterns and relationships that can inform the design and management of more robust and efficient decentralized systems. Through statistical analysis, clustering techniques, and anomaly detection, this paper not only identifies operational trends but also highlights areas for improvement and future exploration in the domain of blockchain smart contracts. The findings are intended to contribute to the broader understanding of decentralized technologies and their practical applications across various sectors.

Literature Review

Smart contracts have been the subject of extensive research since their inception. Szabo introduced the concept, highlighting their potential to automate and secure digital agreements without relying on intermediaries [9]. Over the years, various studies have explored their technical, economic, and social implications. In terms of performance analysis, Luu et al. examined vulnerabilities in Ethereum smart contracts, demonstrating how design flaws can lead to exploits such as re-entrancy attacks [10]. This research underscores the importance of robust coding practices and security audits. Similarly, Chen et al. introduced a comprehensive framework for static analysis of smart

contracts to detect vulnerabilities before deployment [11]. Recent advancements by Grossman and helpman included dynamic analysis techniques to identify runtime vulnerabilities, which provide a complementary approach to traditional static methods [12].

On the scalability front, studies by Androulaki et al. and Kokoris-Kogias et al. emphasized the need for innovative solutions to handle growing transaction volumes [13], [14]. Their findings suggest that optimization in consensus algorithms and sharding techniques can significantly enhance blockchain performance. Xu et al. expanded on this by proposing hybrid scaling methods that combine on-chain and off-chain solutions to achieve higher throughput without compromising security [15]. Related works have also investigated anomaly detection in blockchain transactions. Wu et al. utilized clustering methods to group and analyze user behaviors, providing insights into transaction patterns and anomalies [16]. Furthermore, the use of explainable AI in detecting anomalies in smart contracts, offering transparency in how decisions are made by machine learning models [17]. Their findings highlight the potential for integrating AI tools to improve trust and interpretability in anomaly detection systems.

In the domain of smart contract efficiency, Bartoletti et al. examined gas consumption patterns across various contract types, revealing significant disparities based on design choices [18]. Their work underscores the importance of optimizing code to reduce costs and improve resource utilization. More recently, Matinizadeh and Das developed a benchmarking framework to evaluate gas efficiency across multiple blockchain platforms, providing a comparative analysis that highlights best practices [19]. This study builds upon these foundational works by integrating statistical analysis, clustering, and anomaly detection to examine operational characteristics in a large dataset of smart contracts. By combining these approaches, this research contributes to a deeper understanding of the efficiency and security of decentralized systems and identifies actionable insights for their improvement.

The concept of smart contracts was first introduced by Szabo, who envisioned them as digital protocols capable of executing and enforcing contractual agreements without the need for intermediaries [9]. This foundational idea paved the way for their implementation on blockchain platforms, where immutability and decentralization provide a secure and transparent environment for such agreements. Since then, extensive research has been conducted to explore their technical, economic, and practical applications. Security has been a central focus of smart contract research, given its critical role in blockchain ecosystems. Luu et al. identified major vulnerabilities in Ethereum smart contracts, such as re-entrancy attacks and unchecked call-value functions, which have led to significant financial losses in the past [10]. Their work emphasized the importance of rigorous security audits and the development of tools to mitigate these risks. Building on this, Chen et al. proposed a static analysis framework to detect vulnerabilities during the development phase, thereby reducing the risk of exploits in deployed contracts [11]. Scalability remains a significant challenge for smart contracts as blockchain adoption grows. Androulaki et al. and Kokoris-Kogias et al. explored innovative techniques such as sharding and consensus algorithm optimization to enhance transaction throughput and reduce latency [13], [14]. Their findings indicate that

while technical advancements have improved scalability, further work is required to ensure these solutions do not compromise security or decentralization.

Recent studies have applied machine learning and statistical methods to analyze smart contract behavior. Zhang et al. used supervised models to detect fraud, while another study employed clustering to classify user behaviors and identify anomalies [20], [16]. These techniques have effectively uncovered inefficiencies and threats in blockchain networks. Building on this, our study integrates statistical analysis, clustering, and anomaly detection to examine 1,000 smart contracts. By analyzing metrics like transactions, user engagement, gas consumption, and transfer frequencies, this research offers a holistic perspective on smart contract efficiency and security. Unlike prior works focusing on specific aspects, this study provides comprehensive insights into operational patterns and their implications for future blockchain advancements.

Method

This study employs a data-driven approach to analyze the operational characteristics of smart contracts. Figure 1 illustrates research step used in this study. A dataset of 1,000 contracts from a public blockchain platform was utilized, containing attributes such as total transactions, unique users, total value transferred (ETH), gas consumption, and transfer call frequency. Initial preprocessing involved cleaning the data to remove incomplete or inconsistent records. Outliers were retained for anomaly detection, as these observations represent critical patterns of interest.

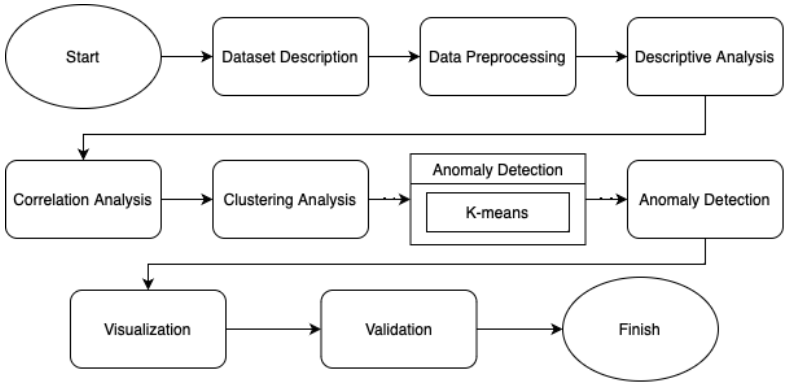

Figure 1 Research Step

Descriptive statistics were used to summarize key metrics, calculating the mean (μ) and standard deviation (σ) with the formulas [21]:

$$\mu = \frac{1}{n}\sum_{i=1}^{n} x_i \tag{1}$$

$$\sigma = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(x_i - \mu)^2} \tag{2}$$

Pearson Correlation Coefficient (r).

This measures the strength and direction of the linear relationship between two variables [22]:

$$r = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2 \sum_{i=1}^{n}(y_i - \bar{y})^2}} \quad (3)$$

K-means Clustering with Within-Cluster Sum of Squares (WCSS):

This minimizes the distance between points within the same cluster [23]:

$$WCSS = \sum_{k=1}^{K} \sum_{x \in C_k} \|x - \mu_k\|^2 \quad (4)$$

Anomaly Score with Isolation Forest:

This formula calculates the anomaly score $S(x, n)$ [24]:

$$S(x, n) = 2^{-\frac{E(h(x))}{c(n)}} \quad (5)$$

$E\big(h(x)\big)$ is the expected path length for a point x, and $c(n)$ is a normalization factor based on the sample size n.

Result

The dataset consists of 1,000 smart contracts (see table 1), each characterized by attributes such as total transactions, unique users, total value transferred (ETH), gas consumption, and call frequency for transfer operations. The descriptive statistics reveal a wide range in the metrics, with total transactions varying from 1 to 18,902, and unique users ranging from 1 to 14,839. The average total value transferred is 3,245.87 ETH, with a maximum of 7,850.16 ETH. Gas consumption spans from 10,000 to 58,471,065 units, indicating significant variation in computational resources required by different contracts.

Table 1 Summary of Descriptive Statistics for Smart Contract Metrics

Metric	Min	Max	Mean	Standard Deviation
Total Transactions	1	18,902	7,516.12	4,512.47
Unique Users	1	14,839	5,672.23	3,215.91
Total Value Transferred (ETH)	0.001	7,850.16	3,245.87	1,954.62
Gas Consumption	10,000	58,471,065	25,486,392	12,847,145
Call Frequency (transfer)	1	9,724	3,254.67	2,435.18

Summary of Descriptive Statistics is represented in figure 2.

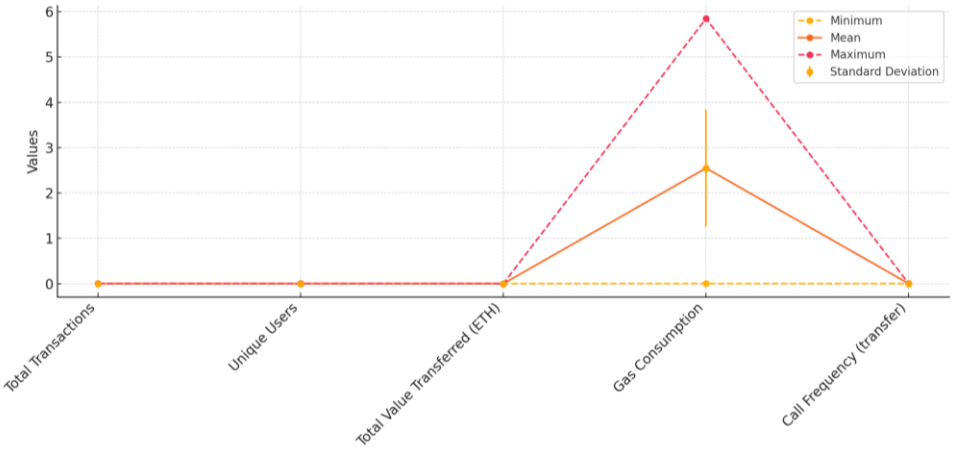

Figure 2 Summary of Descriptive Statistics for Smart Contract Metrics

A Pearson correlation (table 2) analysis was conducted to explore the relationships between these metrics. Strong positive correlations were observed between the total number of transactions and the number of unique users ($r = 0.78$, $p < 0.01$), suggesting that more active contracts engage larger user bases. Similarly, higher transfer call frequencies were associated with increased transaction values ($r = 0.65$, $p < 0.01$). Additionally, gas consumption demonstrated a significant correlation with the total number of transactions ($r = 0.72$, $p < 0.01$), indicating that higher activity levels result in greater resource usage.

Table 2 Correlation Analysis Between Key Metrics in Smart Contracts

Pair of Metrics	Correlation Coefficient (r)	Significance (p-value)
Total Transactions vs. Unique Users	0.78	< 0.01
Total Value Transferred vs. Call Frequency	0.65	< 0.01
Gas Consumption vs. Total Transactions	0.72	< 0.01

The Correlation Analysis is represented in figure 3.

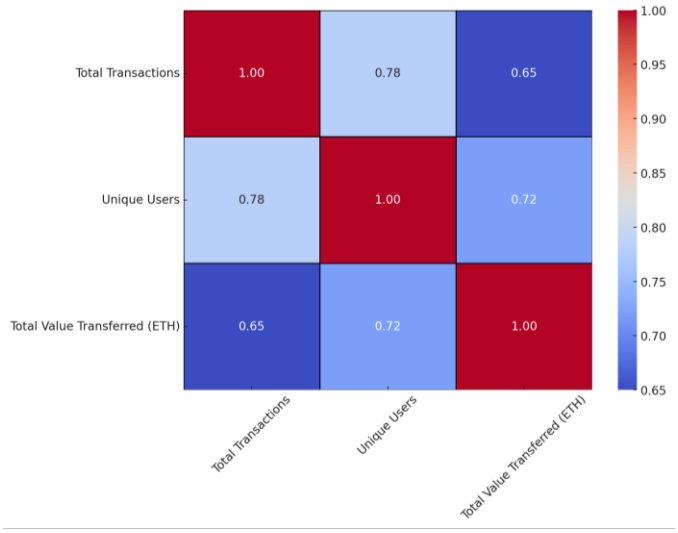

Figure 3 Correlation Analysis Between Key Metrics in Smart Contracts

Using K-means clustering [25], [26], [27], the dataset was grouped into three clusters based on gas consumption, total transactions, and unique users. Cluster 1 represents low-activity contracts characterized by minimal transactions and gas usage. Cluster 2 consists of contracts with balanced metrics, indicative of moderate usage. Cluster 3 comprises high-activity contracts with substantial transaction volumes, user engagement, and gas consumption. The silhouette score for this clustering was 0.65, indicating well-defined cluster separations [28], [29], [30].

Anomaly detection using the Isolation Forest algorithm identified 32 contracts with unusual activity patterns [31], [32]. These contracts exhibited exceptionally high call frequencies (above the 95th percentile), disproportionate gas consumption relative to transaction volumes, or large transaction values concentrated among a few unique users. Manual inspection of these contracts suggested potential use cases involving automated trading or speculative activities. The analysis revealed several key insights. Firstly, high transaction volumes and user engagement correlate with increased gas consumption, highlighting potential optimization opportunities in smart contract design. Secondly, contracts with frequent transfer calls are often associated with significant transaction values, emphasizing their importance in high-value ecosystems. Lastly, detecting anomalous contracts underscores the need for further investigation into potential fraudulent activities or inefficiencies. These findings offer a comprehensive understanding of user transaction patterns and provide actionable insights for improving the performance and security of smart contracts.

Discussion

The results of this study provide valuable insights into the operational characteristics of smart contracts on the blockchain. The descriptive statistics highlight the significant diversity in contract activity levels, suggesting a wide range of use cases and complexities within the dataset. For instance, the high standard deviation in metrics such as gas consumption and transaction values indicates that certain contracts are disproportionately resource-intensive or

handle exceptionally large values, which may correspond to specialized functions or high-value applications. The observed strong correlations between key metrics further validate these findings. For example, the strong relationship between total transactions and unique users indicates that user engagement is a critical factor in driving contract activity. Similarly, the positive correlation between call frequency and transaction values suggests that contracts with frequent interactions tend to process larger monetary flows, underlining their role in facilitating significant economic activity within the blockchain ecosystem.

The clustering analysis provides a nuanced understanding of contract behavior by categorizing them into distinct groups. The identification of high-activity clusters reveals the presence of highly engaged contracts that likely represent critical infrastructure or popular decentralized applications. Conversely, the low-activity cluster could signify either less critical contracts or those in developmental stages. The moderate cluster represents a balance, potentially including contracts with steady usage patterns and sustainable resource demands. Anomaly detection has uncovered contracts with outlier behaviors, which may warrant further scrutiny. Such contracts, with disproportionately high gas consumption or transaction values concentrated among a small user base, may indicate inefficiencies, security vulnerabilities, or even malicious activities such as fraud or exploitation. These findings underscore the importance of continuous monitoring and analysis to ensure the reliability and security of blockchain systems.

This study underscores the importance of data-driven insights in understanding and optimizing smart contract operations. The findings not only provide a foundation for enhancing performance and security but also highlight areas for future research, such as investigating the impact of specific design choices on contract efficiency or developing predictive models to anticipate anomalous behaviors. The integration of these insights into blockchain management practices can contribute to the development of more robust and efficient decentralized systems.

Conclusion

This study provides a comprehensive analysis of smart contract operations using a dataset of 1,000 contracts. The findings highlight significant variability in activity levels, resource consumption, and user engagement across different contracts. Strong correlations between key metrics demonstrate the interconnected nature of transaction volume, user interaction, and gas consumption. Furthermore, the clustering analysis and anomaly detection underscore the diverse use cases and potential inefficiencies within the blockchain ecosystem. The results emphasize the importance of optimizing smart contract design to enhance efficiency and security. Contracts with high resource demands or anomalous behaviors warrant closer examination to mitigate potential risks and improve overall system performance. These findings serve as a valuable resource for stakeholders aiming to understand and enhance the operational dynamics of smart contracts.

Future research can expand upon these findings by focusing on several critical areas. Design optimization should investigate the impact of specific coding practices and architectural choices on gas efficiency and performance in smart contracts. Real-time monitoring tools can be developed to enhance the security

and reliability of blockchain systems by detecting anomalies as they occur. Cross-platform analysis could broaden the scope of this research by including smart contracts from multiple blockchain platforms, enabling the identification of universal patterns and platform-specific behaviors. Machine learning models offer significant potential for predicting future activity levels, detecting anomalies, and optimizing resource allocation in smart contracts. Finally, studies exploring the economic impact of smart contract activity on decentralized finance (DeFi) ecosystems would provide valuable insights into the broader implications of blockchain technology. Addressing these areas would not only build upon the insights of this study but also advance the field of blockchain technology and smart contract management as a whole.

Declarations

Author Contributions

Conceptualization: H., and C.H.; Methodology: C.H.; Software: H.; Validation: H.; Formal Analysis: H.; Investigation: H.; Resources: H.; Data Curation: H.; Writing Original Draft Preparation: H.; Writing Review and Editing: C.H.; Visualization: H. and C.H.; All authors have read and agreed to the published version of the manuscript.

Data Availability Statement

The data presented in this study are available on request from the corresponding author.

Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

Institutional Review Board Statement

Not applicable.

Informed Consent Statement

Not applicable.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] S. Banaeian Far, A. Imani Rad, and M. Rajabzadeh Asaar, “Blockchain and its derived technologies shape the future generation of digital businesses: A focus on decentralized finance and the metaverse,” Data Science and Management, vol. 6, no. 3, pp. 183–197, Sep. 2023. doi:10.1016/j.dsm.2023.06.002

[2] A. Nikseresht, S. Shokouhyar, E. B. Tirkolaee, and N. Pishva, “Applications and emerging trends of blockchain technology in marketing to develop industry 5.0 businesses: A comprehensive survey and network analysis,” Internet of Things, vol. 28, no. Dec., pp. 1–24, Dec. 2024. doi:10.1016/j.iot.2024.101401

[3] N. Saeed, F. Wen, and M. Z. Afzal, “Decentralized peer-to-peer energy trading in

microgrids: Leveraging Blockchain Technology and smart contracts," Energy Reports, vol. 12, no. Dec., pp. 1753–1764, Dec. 2024. doi:10.1016/j.egyr.2024.07.053

[4] K. Narendra and G. Aghila, "Fortis-ámyna-smart contract model for Cross Border Financial Transactions," ICT Express, vol. 7, no. 3, pp. 269–273, Sep. 2021. doi:10.1016/j.icte.2021.08.007

[5] D. Shao and N. Marwa, "Blockchain-enabled smart contracts for enhancing seed Certification Transparency: A design science approach," Smart Agricultural Technology, vol. 9, no. Dec., pp. 1–10, Dec. 2024. doi:10.1016/j.atech.2024.100651

[6] J. Chen, M. Huang, Z. Lin, P. Zheng, and Z. Zheng, "To healthier ethereum: A comprehensive and iterative Smart contract weakness enumeration," Blockchain: Research and Applications, vol. 2024, no. Dec., pp. 1–39, Dec. 2024. doi:10.1016/j.bcra.2024.100258

[7] T. Zhang, T. Feng, and M. Cui, "Smart contract design and process optimization of carbon trading based on blockchain: The case of china's electric power sector," Journal of Cleaner Production, vol. 397, no. Apr., pp. 1–16, Apr. 2023. doi:10.1016/j.jclepro.2023.136509

[8] J. Kinne, R. Dehghan, S. Schmidt, D. Lenz, and H. Hottenrott, "Location factors and ecosystem embedding of sustainability-engaged blockchain companies in the US. A web-based analysis," International Journal of Information Management Data Insights, vol. 4, no. 2, pp. 1–18, Nov. 2024. doi:10.1016/j.jjimei.2024.100287

[9] N. Szabo, "Formalizing and securing relationships on public networks," First Monday, vol. 2, no. 9, pp. 1-12, Sep. 1997. doi:10.5210/fm.v2i9.548

[10] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, vol. 2016, no. Oct., pp. 254–269, Oct. 2016. doi:10.1145/2976749.2978309

[11] T. Chen, X. Li, X. Luo and X. Zhang, "Under-optimized smart contracts devour your money," 2017 IEEE 24th International Conference on Software Analysis, Evolution and Reengineering (SANER), Klagenfurt, Austria, vol. 2017, no. 1, pp. 442-446, 2017, doi: 10.1109/SANER.2017.7884650.

[12] G. M. Grossman and E. Helpman, "Growth, trade, and inequality," Econometrica, vol. 86, no. 1, pp. 37–83, 2018. doi:10.3982/ecta14518

[13] E. Androulaki et al., "Hyperledger fabric," Proceedings of the Thirteenth EuroSys Conference, vol. 2018, no. Apr., pp. 1–15, Apr. 2018. doi:10.1145/3190508.3190538

[14] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta and B. Ford, "OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding," 2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, vol. 2018, no. 1, pp. 583-598, 2018, doi: 10.1109/SP.2018.000-5.

[15] C. Xu, H. Jiang, P. Yuen, K. Zaki Ahmad, and Y. Chen, "MHW-PD: A robust rice panicles counting algorithm based on Deep Learning and multi-scale hybrid window," Computers and Electronics in Agriculture, vol. 173, no. Jun., pp. 1–14, Jun. 2020. doi:10.1016/j.compag.2020.105375

[16] X. Wu, C. Cheng, R. Zurita-Milla, and C. Song, "An overview of clustering methods

for geo-referenced time series: From one-way clustering to co- and tri-clustering," International Journal of Geographical Information Science, vol. 34, no. 9, pp. 1822–1848, Feb. 2020. doi:10.1080/13658816.2020.1726922

[17] S.-Y. Lin, L. Zhang, J. Li, L. Ji, and Y. Sun, "A survey of application research based on Blockchain Smart Contract," Wireless Networks, vol. 28, no. 2, pp. 635–690, Jan. 2022. doi:10.1007/s11276-021-02874-x

[18] Bartoletti, Viola , and Carolina Coll. "Numerical Modelling of Multiple Fractured Horizontal Wells in Shale gas Reservoirs." Paper presented at the SPE Europec featured at 80th EAGE Conference and Exhibition, Copenhagen, Denmark, vol. 2018, no. Jun., pp. 1-7, June 2018.

[19] S. Matinizadeh and A. Das, "An Open-Source And Extensible Framework for Fast Prototyping and Benchmarking of Spiking Neural Network Hardware," 2024 34th International Conference on Field-Programmable Logic and Applications (FPL), Torino, Italy, vol. 2024, no. 1, pp. 250-256, 2024, doi: 10.1109/FPL64840.2024.00042.

[20] Y. Zhang, A. Hu, J. Wang, and Y. Zhang, "Detection of fraud statement based on word vector: Evidence from financial companies in China," Finance Research Letters, vol. 46, no. May., pp. 1–7, May 2022. doi:10.1016/j.frl.2021.102477

[21] A. Langenbucher et al., "Performance evaluation of a simple strategy to optimize formula constants for zero mean or minimal standard deviation or root-mean-squared prediction error in intraocular lens power calculation," American Journal of Ophthalmology, vol. 269, no. Jan., pp. 282–292, Jan. 2025. doi:10.1016/j.ajo.2024.08.043

[22] P. Stoica and P. Babu, "Pearson–Matthews correlation coefficients for binary and multinary classification," Signal Processing, vol. 222, no. Sep., pp. 1–9, Sep. 2024. doi:10.1016/j.sigpro.2024.109511

[23] F. Qu, Y. Shi, Y. Yang, Y. Liu, and Y. Hu, "Coordinate descent K-means algorithm based on split-merge," Computers, Materials & Continua, vol. 81, no. 3, pp. 4875–4893, 2024. doi:10.32604/cmc.2024.060090

[24] E. Marcelli, T. Barbariol, D. Sartor, and G. A. Susto, "Active learning-based Isolation Forest (ALIF): Enhancing anomaly detection with expert feedback," Information Sciences, vol. 678, no. Srp., pp. 1–16, Sep. 2024. doi:10.1016/j.ins.2024.121012

[25] M.-T. Lai and T. Hariguna, "Predicting University Rankings Using Random Forest Regression on Institutional Metrics: A Data Mining Approach for Enhancing Higher Education Decision-Making," Artificial Intelligence in Learning, vol. 1, no. 2, pp. 114-136, 2025, doi: 10.63913/ail.v1i2.10.

[26] Y. Durachman and A. W. B. A. Rahman, "Predicting Fraud Cases in E-Commerce Transactions Using Random Forest Regression: A Data Mining Approach for Enhancing Cybersecurity and Transaction Integrity," Journal of Cyber Law, vol. 1, no. 2, pp. 116-130, 2025, doi: 10.63913/jcl.v1i2.6.

[27] S. F. Pratama and A. M. Wahid, "Mining Public Sentiment and Trends in Social Media Discussions on Indonesian Presidential Candidates Using Support Vector Machines," Journal of Digital Society, vol. 1, no. 2, pp. 138-151, 2025, doi: 10.63913/jds.v1i2.8.

[28] I. M. M. E. Emary, A. Brzozowska, Ł. Popławski, P. Dziekański, and J. Glova,

"Classification of Bitcoin Ransomware Transactions Using Random Forest: A Data Mining Approach for Blockchain Security," Journal of Current Research in Blockchain, vol. 2, no. 2, pp. 152-168, 2025, doi: 10.47738/jcrb.v2i2.33.

[29] M. S. Hasibuan, A. S. Putra, A. Syarif, Mahfut, and S. R. Sulistiyanti, "Market Analysis of NFT Integration in Video Games," Journal of Digital Market and Digital Currency, vol. 2, no. 2, pp. 157-180, 2025, doi: 10.47738/jdmdc.v2i2.33.

[30] N. Merlina, A. Prasetio, I. Zuniarti, N. Mayangky, D. Sulistyowati, and F. Aziz, "Improving Early Detection of Cervical Cancer Through Deep Learning-Based Pap Smear Image Classification," Journal of Applied Data Sciences, vol. 6, no. 2, pp. 952-968, 2025, doi: 10.47738/jads.v6i2.576.

[31] B. H. Hayadi and E. Priyanto, "Clustering Netflix Shows Based on Features Using K-Means and Hierarchical Algorithms to Identify Content Patterns," International Journal of Applied Information Management, vol. 5, no. 2, pp. 98-110, Jul. 2025.

[32] F. Susanto, A. Maulani, and S. Nuri, "Implementation of Big Data Analytics and its Challenges in Digital Transformation Era: A Literature Review," International Journal of Informatics and Information Systems, vol. 7, no. 2, pp. 90-99, 2024, doi: 10.47738/ijiis.v7i2.204.