Journal of Accounting, Entrepreneurship, and Financial Technology (JAEF) p-ISSN: 2686 - 4479
Volume 07, Number 02, April 2026 e-ISSN: 2686 - 5505

Digital Transformation and Corruption Control: Unveiling the Paradox of Cybersecurity in Global Governance

Nicholas Chang*
Universitas Ciputra Surabaya

Abstract: This study examines the association between digital transformation, represented by blockchain, e-government, and cybersecurity, and corruption, proxied by the Corruption Perceptions Index (CPI), within the framework of good governance and Sustainable Development Goal 16. Using a quantitative approach, this study analyzes secondary data from 23 countries characterized by relatively high levels of blockchain adoption. Multiple linear regression analysis was employed using SPSS version 27. The results indicate that blockchain and e-government are positively and significantly associated with CPI, suggesting that higher levels of digital readiness tend to coincide with lower perceived corruption within the sample. E-government shows the strongest association within the model, which is consistent with its potential relevance to transparency, accountability, and public service efficiency. In contrast, cybersecurity is negatively and significantly associated with CPI, indicating that stronger cybersecurity capacity does not necessarily correspond to lower perceived corruption and may reflect tensions between control and transparency when not supported by appropriate governance frameworks. These findings suggest that digital transformation alone is insufficient to combat corruption. Its effectiveness depends on alignment with good governance principles, particularly transparency and accountability. This study contributes by providing an integrated perspective on digital transformation and offers implications for policymakers in designing balanced digital governance strategies.

Keywords: blockchain, e-government, cybersecurity, corruption, good governance

Received: *24 March 2026,* ***Revised:*** *11 April 2026,* ***Accepted:*** *19 April 2026*

*Corresponding Author.
Email: nicholaschang01@student.ciputra.ac.id

INTRODUCTION

Sustainable development transcends environmental and economic concerns, emphasizing justice, institutional integrity, and societal inclusiveness. Within this framework, Goal 16 of the Sustainable Development Goals (SDGs) explicitly underscores the imperative of combating corruption to foster peaceful and inclusive societies (Hope, 2020; Bozhenko et al., 2023). Nevertheless, corruption persists as a formidable and systemic barrier to these mandates. According to Transparency International (2024), the global average of the Corruption Perceptions Index (CPI) has stagnated at 43 out of 100 for five consecutive years, signifying negligible progress in curbing malfeasance. This stagnation reflects a global prevalence of corrupt practices that catalyze financial instability, exacerbate economic disparity, and stifle investment (Mehawesh & Al-Badayneh, 2025; Arwati & Latif, 2019).

In response to these protracted challenges, governments have increasingly pivoted toward digital transformation as a strategic lever for enhancing governance quality. The deployment of digital architectures, particularly e-government systems, is intended to bolster transparency, optimize public service delivery, and invigorate civic engagement (Alaa & Misko, 2022; Sohag et al., 2021). Paradoxically, empirical evidence suggests that widespread digitalization does not invariably translate into diminished corruption. This phenomenon challenges the deterministic assumption that technological advancement inherently fosters integrity. Recent scholarship indicates that despite extensive e-government integration, numerous jurisdictions have seen no significant decline in corrupt activities (Seiam & Salman, 2024), a situation often compounded by flagging institutional commitment and a lack of structural reforms (Thanh et al., 2025; Dang et al., 2025).

To resolve this paradox, various emerging technologies have been proposed as remedial instruments, most notably blockchain. Offering a decentralized and immutable ledger, blockchain minimizes avenues for data manipulation, fraud, and collusion, thereby refining accountability in the public sector (Ramadani et al., 2023; Cagigas et al., 2021). Furthermore, it has demonstrated potential in revolutionizing service delivery through highly auditable governance frameworks (Ølnes et al., 2017; Handoko et al., 2024).

However, heightened reliance on digital ecosystems introduces critical vulnerabilities, particularly concerning cybersecurity. With global internet penetration reaching 5.65 billion users (Data Reportal, 2025), digital systems face unprecedented threats. Cybersecurity thus emerges as a prerequisite for safeguarding data integrity against unauthorized access (Javaid

et al., 2023; Suryayusra et al., 2025). Crucially, robust security protocols can detect fraudulent deviations in real-time, positioning cybersecurity as a strategic deterrent against corruption rather than a mere technical safeguard (Dobrovolska & Rozhkova, 2024; Abbas et al., 2022). Absent these measures, government portals remain susceptible not only to external breaches but also to internal subversion, where authorized actors might exploit systemic flaws to obfuscate illicit activities.

While e-government remains a cornerstone of digital reform by curtailing the face-to-face interactions prone to bribery (Dang et al., 2025; Kalesnikaite et al., 2023), the efficacy of these combined technologies, blockchain, cybersecurity, and e-government remains inconsistent globally. This inconsistency reveals a significant research lacuna; previous inquiries have largely scrutinized these technologies in isolation, leading to fragmented insights (Trequattrini et al., 2024; Ajibade & Mutula, 2022). Moreover, cybersecurity's role as a core governance mechanism, rather than a technical adjunct remains under-researched.

Addressing these gaps, this study investigates whether the synergistic adoption of the Blockchain Readiness Index (BRI), Cybersecurity Index (CI), and E-Government Development Index (EGDI) effectively mitigates corruption on a global scale. By integrating these dimensions into a unified analytical framework, the research seeks to provide a holistic understanding of digital transformation's role in fortifying institutional integrity, ultimately offering actionable insights for achieving the transparency and accountability envisioned in SDG 16.

This study is grounded in Good Governance Theory, which explains corruption as an institutional consequence of weak transparency, limited accountability, ineffective control, and excessive administrative discretion. In this perspective, governance quality improves when public decision-making becomes more transparent, rule-based, auditable, and subject to oversight (Addink, 2018; United Nations Development Programme, 1997; Nur et al., 2025). Therefore, the relevance of digital transformation to corruption control lies not in technology itself, but in whether it strengthens these governance mechanisms.

Based on this logic, blockchain, e-government, and cybersecurity are treated as distinct governance instruments rather than merely indicators of digital modernization. Each variable affects corruption through a different institutional pathway. Blockchain is associated with traceability and immutability, e-government with procedural standardization and reduced direct discretion, and cybersecurity with data integrity and system reliability

(Trequattrini et al., 2024; World Economic Forum, 2020; Ramadani et al., 2023; Lee et al., 2020; Munari, 2024; Malodia et al., 2021; Javaid et al., 2023; Suryayusra et al., 2025). Thus, Good Governance Theory provides the analytical link between digital transformation and corruption by focusing on how technology reshapes transparency, accountability, and institutional control.

Blockchain is fundamentally defined as a decentralized, distributed digital ledger that facilitates the secure and immutable documentation of transactions (Trequattrini et al., 2024; World Economic Forum, 2020; Bhaskar et al., 2020). From a good governance perspective, its anti-corruption relevance lies in its ability to create permanent and verifiable records, thereby reducing the possibility of ex post manipulation, document alteration, and collusive intervention in administrative processes (Ramadani et al., 2023; Lee et al., 2020). In governance terms, blockchain strengthens transparency by making transactions traceable and strengthens accountability by making administrative actions easier to audit.

This mechanism is particularly relevant in corruption-prone areas such as procurement, licensing, and public records, where abuse often depends on weak documentation and fragmented oversight. Prior studies show that blockchain can support accountability and improve the integrity of public service systems, especially where verification and traceability are central requirements (Ølnes et al., 2017; Handoko et al., 2024; Cagigas et al., 2021; Kim & Kang, 2021). Accordingly, higher blockchain readiness is expected to be associated with stronger corruption control.

H1: Blockchain is positively associated with the Corruption Perceptions Index.

E-government refers to the use of Information and Communication Technology (ICT) to improve the efficiency and accountability of public service delivery (Munari, 2024; Malodia et al., 2021). Within Good Governance Theory, its importance lies in reducing opaque face-to-face interaction, standardizing procedures, and increasing the visibility of administrative processes. Corruption often emerges when public officials exercise broad discretion in settings characterized by procedural ambiguity and informal exchange. By digitalizing services, e-government narrows such discretionary space and records administrative interactions more systematically (Dobrovolska & Rozhkova, 2024).

In this way, e-government contributes to transparency, accountability, and procedural consistency. It allows citizens to access clearer information, reduces opportunities for bribery in direct encounters, and improves the auditability of public service transactions. Previous studies consistently suggest that e-government can reduce corruption when digital systems

simplify procedures and strengthen institutional monitoring (Dang et al., 2025; Rustiarini, 2019; Kalesnikaite et al., 2023; Sugiarti & Akbar, 2024). Therefore, stronger e-government development is expected to correspond with lower perceived corruption.
H2: E-Government is positively associated with the Corruption Perceptions Index.

Cybersecurity constitutes the set of measures designed to protect digital systems from unauthorized access, disruption, and manipulation (Javaid et al., 2023; Suryayusra et al., 2025). In the context of digital governance, this function is essential because transparency and accountability depend on the integrity of digital records and information systems. If public data can be altered, deleted, or exploited, then digital governance cannot reliably support corruption control.

From a good governance perspective, cybersecurity strengthens institutional control by protecting audit trails, preserving data credibility, and reducing the risk of manipulation by internal or external actors (Abbas et al., 2022). At the same time, its role is more complex than that of blockchain or e-government because security can also be associated with restricted access and reduced openness if not balanced by accountability safeguards. This is why cybersecurity should be understood not merely as a technical necessity, but as a governance mechanism whose anti-corruption effect depends on how it is institutionally embedded (Zubaedah et al., 2024; Mittelstadt et al., 2016). Nevertheless, under the assumption that secure systems are necessary for reliable oversight, stronger cybersecurity is expected to support corruption control.
H3: Cybersecurity is positively associated with the Corruption Perceptions Index.

Overall, the three variables represent complementary dimensions of digital governance. Blockchain strengthens the credibility of records, e-government improves the structure of administrative interaction, and cybersecurity protects the integrity of the digital environment in which governance operates (Trequattrini et al., 2024; World Economic Forum, 2020; Ølnes et al., 2017; Cagigas et al., 2021; Munari, 2024; Malodia et al., 2021; Dang et al., 2025; Kalesnikaite et al., 2023; Javaid et al., 2023; Abbas et al., 2022; Zubaedah et al., 2024). Their common relevance to corruption lies in the extent to which they reinforce the principles of transparency, accountability, and effective oversight emphasized by Good Governance Theory (Addink, 2018; United Nations Development Programme, 1997; Nur et al., 2025).

METHODS

Data Types and Source

This study employs a quantitative design using secondary data from 23 countries identified as having relatively high levels of blockchain adoption (Henley & Partners, 2023). This purposive sampling was intended to focus the analysis on countries with relatively advanced digital transformation profiles and comparable data availability across the selected indicators. The dependent variable, corruption, is defined as the misappropriation of public authority and proxied by the Corruption Perceptions Index (CPI, 0–100), where higher scores indicate greater institutional integrity (Transparency International, 2023).

The analytical framework incorporates three independent variables representing digital maturity: Blockchain, measured via the Blockchain Readiness Index (BRI, 0–60) across six dimensions including regulation and infrastructure; E-Government, assessed through the E-Government Development Index (EGDI, 0–1) based on online services, telecommunications, and human capital (World Bank, 2023a); and Cybersecurity, quantified by the Cybersecurity Index (CI, 0–100) across five pillars including legal and technical frameworks (World Bank, 2023b). Collectively, these indicators provide an empirical basis for examining the relationship between dimensions of digital transformation and governance quality.

Data Analysis Methods

This study employs multiple linear regression to examine the association between the selected dimensions of digital transformation and CPI, using SPSS version 27 for data processing. The analytical procedure commences with the computation of descriptive statistics to elaborate on the fundamental characteristics and distributional trends of each variable. To ensure the robustness and reliability of the econometric model, a rigorous suite of diagnostic tests is implemented. Given the relatively constrained sample size ($N < 50$), the normality of the dataset is verified via the Shapiro–Wilk method (Ningsih et al., 2019), while potential multicollinearity is scrutinized through Variance Inflation Factor (VIF) and tolerance thresholds (Sriningsih et al., 2018; Adijaya & Radianto, 2025). Furthermore, homoscedasticity is assessed using the Glejser technique to identify any variance inconsistencies within the residuals (Ilori & Tanimowo, 2022). Upon the fulfillment of these diagnostic prerequisites, multiple linear regression is deployed to determine the predictive

influence of blockchain readiness, e-government development, and cybersecurity capacity on corruption perceptions. The research model is mathematically expressed as:

$$Y = \alpha + \beta 1X1 + \beta 2X2 + \beta 3X3 + \varepsilon$$

Where Y represents the Corruption Perceptions Index (CPI), α denotes the constant, $\beta 1 - \beta 3$ signify the regression coefficients for the respective independent variables, and ε constitutes the error term capturing exogenous variance. This statistical approach is intended to identify patterns of association between the selected digital variables and CPI within the scope of the available data.

RESULTS

Descriptive Statistics

As evidenced by the descriptive statistics in Table 1, the Corruption Perceptions Index (Y), serving as the proxy for institutional integrity, yields a mean value of 62.739 with a standard deviation of 15.383. This indicates that while the sampled jurisdictions generally exhibit relatively favorable levels of perceived transparency, the substantial standard deviation underscores significant cross-country disparities in governance quality. Regarding technological readiness, the Blockchain (X1) records a moderate mean of 36.211. The relatively narrow dispersion of values—ranging from 24.80 to 50.20 with a standard deviation of 6.933—suggests that most countries in the cohort are at a comparable stage of blockchain infrastructural development.

Furthermore, the E-Government (X2) demonstrates a high mean of 0.821 (SD = 0.105), suggesting that a majority of the analyzed nations have reached an advanced echelon of digital governance, particularly regarding online service frameworks and human capital. In contrast, the Cybersecurity (X3) exhibits the highest average score at 87.123; however, the elevated standard deviation of 22.774 reveals notable polarizations in cybersecurity capacity among the nations. Collectively, these findings highlight a landscape where digital infrastructure is broadly sophisticated, yet national preparedness for cybersecurity remains inconsistent.

Table 1 Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Y	23	34.00	85.00	62.739	15.383
X1	23	24.80	50.20	36.211	6.933
X2	23	0.53	0.94	0.821	0.105
X3	23	18.20	100.00	87.123	22.774
Valid N (listwise)	23				

Classical Assumption Test

The normality of the dataset was evaluated using the Shapiro–Wilk test, a method specifically selected for its superior sensitivity in analyzing sample sizes smaller than 50 (Mishra et al., 2019). As illustrated by the empirical results in Table 2, all studied variables demonstrated significance values exceeding the 0.05 threshold, specifically 0.112, 0.856, 0.348, and 0.828, respectively. These results indicate that all variables have significance values above 0.05, suggesting that the data do not significantly deviate from normality. Accordingly, the normality assumption for the regression model is considered acceptable.

Table 2 Normality Test

	Statistic	df	Sig.
Y	0.909	16	0.112
X1	0.971	16	0.856
X2	0.940	16	0.348
X3	0.969	16	0.828

Multicollinearity diagnostics were executed utilizing both tolerance levels and Variance Inflation Factor (VIF) metrics to ensure the structural integrity of the model. As illustrated in Table 3, the tolerance values for Blockchain (X1), E-Government (X2), and Cybersecurity (X3) consistently surpassed the critical threshold of 0.01. Correspondingly, all VIF values—specifically 1.530, 2.340, and 1.849—remained substantially below the conservative maximum limit of 10. These results suggest that multicollinearity is not a substantial concern in the model, as all tolerance and VIF values remain within commonly accepted thresholds (Binus, 2021). Consequently, the distinct influence of each predictor on corruption perceptions can be interpreted with a high degree of statistical reliability.

Table 3 Multicollinearity Test

Variable	Tolerance	VIF
X1	0.654	1.530
X2	0.427	2.340
X3	0.541	1.849

The diagnostic for heteroscedasticity was executed utilizing the Glejser method to ensure the stability of the model's error variance. As delineated in Table 4, the p-values for Blockchain (X1), E-Government (X2), and Cybersecurity (X3) all significantly surpassed the 0.05 alpha level. These results indicate no statistically significant relationship between the independent variables and the absolute residuals, suggesting that heteroscedasticity is not evident in the model. Consequently, it can be inferred that the residuals maintain a constant variance across all levels of the predictor variables, successfully satisfying the homoscedasticity assumption essential for reliable regression estimates (Karina et al., 2023).

Table 4 Heteroscedasticity Test

Variable	t	Sig.
(Constant)	0.008	0.994
X1	0.874	0.393
X2	0.170	0.866
X3	1.541	0.140

Statistical Test

As shown in Table 5, the model is statistically significant overall, with a Prob > F value of less than 0.001. This indicates that the three independent variables are jointly associated with CPI within the estimated model. Furthermore, the coefficient of determination yields a value of 0.640, indicating that 64% of the variance in the Corruption Perceptions Index (CPI) can be explained by the integrated digital transformation variables, while the remaining 36% is attributed to exogenous factors beyond the current analytical scope. The Adjusted R Square of 0.584 suggests that the model retains a moderate level of explanatory capacity after accounting for the number of predictors and sample size. Additionally, the multiple correlation coefficient (R) of 0.800 indicates a relatively strong linear association

within the sample, while the Standard Error of the Estimate of 9.926 reflects the average prediction error of the model.

Table 5 Coefficient of Determination and F-Test

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Prob > F
1	0.800	0.640	0.584	9.926	<0.001

Based on the multiple regression results shown in Table 6, blockchain, e-government, and cybersecurity each show statistically significant associations with CPI, although the directions of those associations differ. Blockchain shows a positive and significant association with CPI, with a coefficient of 0.810 and a significance value of 0.038. This indicates that higher blockchain readiness in the sample is associated with higher CPI scores, which correspond to lower perceived corruption. Therefore, Hypothesis 1 (H1), which proposes a positive association between blockchain readiness and CPI, is supported.

E-government shows the strongest positive association within the model, with a coefficient of 127.615, a significance value of 0.002, and a standardized beta of 0.776. This result suggests that higher levels of e-government development are associated with higher CPI scores, a pattern that is consistent with the argument that digital public service systems may support transparency and governance quality. Thus, Hypothesis 2 (H2) is also supported. In contrast, cybersecurity shows a negative and significant association with CPI, with a coefficient of -0.629 and a significance value of 0.007. This indicates that higher cybersecurity capacity in the sample is associated with lower CPI scores, which correspond to higher perceived corruption. Therefore, Hypothesis 3 (H3), which proposes a positive association between cybersecurity and CPI, is not supported because the observed relationship is negative.

Table 6 Multiple Linear Analysis

Variable	B	Std. Error	Beta	t	Sig.
(Constant)	-15.779	19.231		-0.820	0.422
BRI	0.810	0.363	0.380	2.230	0.038
EGDI	127.615	34.597	0.776	3.689	0.002
CI	-0.629	0.209	-0.564	-3.014	0.007

DISCUSSION

The findings of this study suggest that digital transformation is associated with corruption through different governance pathways rather than through a single uniform mechanism. Interpreted through Good Governance Theory, this pattern is important because corruption is typically rooted in weak transparency, limited accountability, and insufficient constraints on administrative discretion (Addink, 2018; Mittelstadt et al., 2016). In that sense, blockchain, e-government, and cybersecurity should not be understood merely as technological indicators, but as institutional instruments that may shape the quality of governance in different ways. Although these findings should be interpreted with appropriate caution given the study's limited sample, cross-sectional design, and absence of control variables, they still offer a meaningful analytical contribution by showing that the anti-corruption relevance of digital transformation depends on how specific technologies interact with the core principles of governance rather than on digitalization alone.

The positive association between blockchain and CPI indicates that countries with higher blockchain readiness in this sample also tend to report better corruption perceptions. This pattern is broadly consistent with Good Governance Theory, especially the argument that stronger transparency and accountability are associated with better institutional outcomes (Addink, 2018; Mittelstadt et al., 2016). A plausible explanation lies in blockchain's capacity to strengthen the immutability and traceability of records, thereby making administrative intervention more visible and ex post manipulation more difficult (Ohize et al., 2024; Senarathna, 2025). From this perspective, blockchain is relevant not because it is technologically advanced in itself, but because it may reduce information asymmetry and narrow the space for discretionary abuse in governance processes. This interpretation is aligned with earlier arguments that blockchain can reinforce institutional integrity when embedded in accountability-oriented governance arrangements (Aarvik, 2020; Normand, 2025). Thus, the contribution of this finding is not to claim that blockchain automatically reduces corruption, but to indicate that the governance value of blockchain lies in its potential to convert transparency from a formal principle into a more auditable administrative practice.

A comparable interpretation applies to e-government, which shows the strongest positive association with CPI among the three variables. This result is also broadly consistent with Good Governance Theory, but it points to a somewhat different mechanism. Whereas blockchain mainly concerns the credibility of records, e-government is more directly related

to the restructuring of administrative interaction. Corruption often persists where bureaucratic procedures are opaque, service standards are inconsistently applied, and face-to-face contact creates room for informal bargaining. E-government may weaken these conditions by converting informal exchanges into rule-based digital procedures, reducing procedural ambiguity and limiting discretionary contact between officials and citizens. This helps explain why e-government in this study appears more strongly associated with CPI than blockchain: its relevance is situated not only at the level of information integrity but also at the level of everyday public service delivery. Such an interpretation is consistent with studies showing that digital public services may strengthen accountability, efficiency, and transparency by simplifying procedures and improving monitoring capacity (Jafar, 2024; Baum & Potter, 2019; Hochstetter et al., 2023). It also accords with the argument that real-time digital interaction can expand oversight and strengthen institutional trust, both of which are central to SDG 16 (Nookhao & Kiattisin, 2023; Sukarno et al., 2024). Therefore, this finding usefully suggests that within the broader architecture of good governance, the reduction of opaque and discretionary interaction may be one of the most consequential channels linking digital reform to corruption control.

The cybersecurity result, however, introduces a more complex pattern because its negative association with CPI does not follow the same direction as the initial hypothesis. Rather than treating this as a simple contradiction, the finding is more productively read as revealing an internal tension within Good Governance Theory itself. In principle, cybersecurity should support good governance because reliable oversight depends on the integrity, security, and continuity of digital systems. Prior studies indeed argue that cybersecurity can protect information infrastructures from unauthorized manipulation and preserve the credibility of administrative data (Li & Liu, 2021; Katrakazas et al., 2020). Yet the present result suggests that stronger cybersecurity capacity does not necessarily correspond to better corruption perceptions in a linear way. One possible explanation is that cybersecurity may strengthen the control dimension of governance while not always strengthening, and in some cases potentially constraining, the transparency dimension. Where security frameworks are implemented in highly restrictive or centralized forms, they may reduce external scrutiny, limit access to information, or create institutional opacity. This interpretation is supported by literature suggesting that cybersecurity arrangements can be used in ways that restrict oversight when governance safeguards are weak (Sakhnini et al., 2021). Under that reading, the negative coefficient does not mean that cybersecurity is inherently detrimental to governance, but rather that its anti-corruption value is conditional

on whether security is balanced with openness, answerability, and accountability. This is precisely where the study adds analytical value: it suggests that not all governance-enhancing technologies work through the same institutional logic, and that some may generate trade-offs when one principle of good governance is strengthened at the expense of another.

Taken together, these results suggest that the relationship between digital transformation and corruption is better understood as conditional, differentiated, and governance-mediated. Blockchain and e-government appear broadly aligned with the expectations of Good Governance Theory because both are associated with mechanisms that enhance transparency and reduce discretionary abuse, although they do so through different institutional channels. Cybersecurity, by contrast, highlights that governance is not simply a matter of adding more control capacity. Instead, effective anti-corruption governance requires a balance between transparency, accountability, and protection of institutional integrity. In this sense, blockchain may be associated with the credibility of records, e-government with the procedural structuring of administrative interaction, and cybersecurity with the safeguarding of digital infrastructures on which governance increasingly depends (Mensah, 2020; Mamulak et al., 2024). However, these dimensions should not be assumed to reinforce one another automatically. As previous studies note, transparency without adequate security may expose systems to manipulation, while security without sufficient transparency may produce opacity (Lykidis et al., 2021). The broader implication is that digital transformation should not be conceptualized as a singular anti-corruption remedy, but as a set of governance tools whose effectiveness depends on institutional alignment.

Overall, this study provides a useful contribution to the literature by showing that Good Governance Theory remains relevant for interpreting digital anti-corruption strategies, but that its application in the digital era must be more nuanced. The results are broadly consistent with the proposition that corruption control depends on transparency, accountability, and effective oversight, yet they also suggest that these principles may interact in more complex ways when mediated by different technologies (Azmi & Nugroho, 2023; El Kafhali, 2024). The contribution of the study, therefore, lies not in making definitive causal claims, but in offering a more differentiated reading of how blockchain, e-government, and cybersecurity relate to corruption through distinct governance logics. In the context of SDG 16, this implies that digital reform should be assessed not only in terms of technological

expansion, but in terms of whether it produces a governance configuration capable of sustaining openness, control, and public trust at the same time.

Conclusion, Limitations, and Suggestions

This study examines the association of blockchain, e-government, and cybersecurity with corruption, proxied by the Corruption Perceptions Index (CPI), within the framework of Good Governance Theory and digital transformation. The findings show that blockchain and e-government are positively and significantly associated with CPI, indicating that countries with higher blockchain readiness and stronger e-government development in this sample also tend to display lower perceived corruption. By contrast, cybersecurity is negatively and significantly associated with CPI, suggesting that stronger cybersecurity capacity does not necessarily correspond to better corruption perceptions. These findings indicate that digital transformation should not be understood as a single or uniformly beneficial governance intervention. Rather, its relevance to corruption control depends on the specific institutional mechanism through which each technological dimension operates.

From a theoretical perspective, this study supports the relevance of Good Governance Theory, particularly its emphasis on transparency, accountability, and institutional control as core conditions for reducing corruption. At the same time, the findings show that these principles do not operate in a simple linear manner in the context of digital governance. Blockchain and e-government are broadly consistent with the expectation that corruption becomes less likely when governance systems are more traceable, auditable, and less dependent on discretionary interaction. However, the cybersecurity result suggests that stronger control capacity alone is insufficient when it is not balanced with openness and external scrutiny. In this sense, the study contributes by offering a more differentiated analytical reading of digital governance: blockchain is associated with the credibility of records, e-government with the restructuring of administrative interaction, and cybersecurity with the protection of digital systems whose governance value depends on their alignment with broader institutional principles.

From a practical and policy perspective, the study implies that governments should approach digital reform not merely as technological expansion, but as institutional design. E-government appears especially relevant because it is associated with the standardization of procedures and the reduction of corruption-prone discretionary interaction in public service delivery. Blockchain also holds importance insofar as it may strengthen traceability and

auditability in administrative areas vulnerable to manipulation, such as procurement, records management, and public transactions. Cybersecurity, meanwhile, should not be treated solely as a technical objective, but as part of a governance framework that must protect data integrity without undermining transparency, accountability, and public trust. Therefore, in the context of SDG 16, the main implication of this study is that anti-corruption-oriented digital transformation requires a balanced integration of openness, control, and institutional reliability in order to support more transparent, accountable, and corruption-resistant governance systems.

This study has several limitations that should be considered when interpreting the findings. First, the analysis relies entirely on secondary data obtained from international institutions such as Transparency International, the World Bank, and Henley & Partners. Although these sources are widely recognized, differences in data collection methods, measurement approaches, and reporting periods may introduce inconsistencies that cannot be fully controlled. Second, the study is based on a relatively small sample of countries, constrained by data availability and compatibility across all variables, which may limit the generalizability of the findings, particularly for countries with different levels of digital development or institutional characteristics. Third, the regression model does not incorporate control variables, meaning that the observed relationships between blockchain, e-government, cybersecurity, and corruption should be interpreted as associative rather than causal. Other relevant factors such as economic development, political stability, or institutional quality, may also influence corruption but are not captured within the current model. Taken together, these limitations suggest that the findings should be interpreted cautiously, while still offering indicative insights into the relationship between digital transformation and corruption within the scope of the data used.

Governments should prioritize the development of e-government and blockchain-based governance mechanisms in administrative areas that are highly vulnerable to corruption, particularly public procurement, budget administration, licensing, and asset management. The rationale is not merely technological modernization, but the institutional capacity of these systems to strengthen procedural standardization, transaction traceability, and auditability. In this way, digital reform can more effectively reduce discretionary intervention and improve accountability in corruption-prone public processes.

With regard to cybersecurity, policy development should move beyond technical reinforcement alone. Cybersecurity frameworks need to be designed in a way that protects

data integrity and system reliability without weakening transparency, public scrutiny, or access to information. This means that security policies should be accompanied by clear governance safeguards, including accountability mechanisms, oversight arrangements, and regulatory standards that prevent the concentration of informational control.

More broadly, governments need to ensure that digital transformation is implemented as part of a coherent governance strategy rather than as isolated technological adoption. This requires clear communication regarding the purpose and public value of digital systems, as well as the strengthening of participatory and oversight mechanisms that sustain public trust. Accordingly, a balanced integration of blockchain, e-government, and cybersecurity within a good governance framework may provide a more credible basis for strengthening anti-corruption efforts and advancing the institutional objectives of SDG 16.

REFERENCES

Aarvik, P. (2020). *Blockchain as an Anticorruption Tool*. Oslo: CMI.

Abbas, H. S. M., Qaisar, Z. H., Xu, X., & Sun, C. (2022). Nexus of E-government, Cybersecurity and Corruption on Public Service (PSS) Sustainability in Asian Economies Using Fixed-Effect and Random Forest Algorithm. *Online Information Review*, *46*(4), 754–770. https://doi.org/10.1108/OIR-02-2021-0069

Addink, G. H. (2018). Good Governance: Importance in Practice, Theories and Definitions. *Halu Oleo Law Review*, *1*(1), 1–32. https://doi.org/10.33561/holrev.v1i1.2347

Adijaya, V., & Radianto, E. D. W. (2025). Debt, Profit, and Tax: Investigating Corporate Tax Behavior. *Journal of Accounting, Entrepreneurship and Financial Technology (JAEF)*, *7*(1), 55–74. https://doi.org/10.37715/jaef.v7i1.6069

Ajibade, P., & Mutula, S. M. (2022). The Use of Blockchain Technology in Electronic Records Management Systems to Mitigate Corruption in South Africa. *Mousaion: South African Journal of Information Studies*, *39*(4), 1–19. https://doi.org/10.25159/2663-659X/10149

Alaa, D., & Misko, O. (2022). The Digitalization and its Influence on Combating Corruption. *Public Administration and Civil Service*, *1(80)*, 183–197. https://doi.org/10.52123/1994-2370-2022-570

Arwati, D., & Latif, D. V. (2019). Tingkat Kepercayaan Masyarakat terhadap Transparansi Keuangan dalam E Government Kota Bandung. *JBMP (Jurnal Bisnis, Manajemen dan Perbankan)*, *5*(2), 66–74. https://doi.org/10.21070/JBMP.V5I2.2736

Azmi, I. F., & Nugroho, A. A. (2023). Anti-Corruption System 4.0: The Adoption of Blockchain Technology in the Public Sector. *Integritas : Jurnal Antikorupsi*, *9*(1), 93–108. https://doi.org/10.32697/integritas.v9i1.985

Baum, M. A., & Potter, P. B. K. (2019). Media, Public Opinion, and Foreign Policy in the Age of Social Media. *Journal of Politics*, *81*(2), 747–756. https://doi.org/10.1086/702233

Bhaskar, P., Tiwari, C. K., & Joshi, A. (2020). Blockchain in Education Management: Present and Future Applications. *Interactive Technology and Smart Education*, *18*(1), 1–17. https://doi.org/10.1108/ITSE-07-2020-0102

Binus. (2021). *Memahami Uji Multikolinearitas dalam Model Regresi – Accounting*. https://accounting.binus.ac.id/2021/08/06/memahami-uji-multikolinearitas-dalam-model-regresi.

Bozhenko, V., Boyko, A., & Voronenko, I. (2023). Corruption as an Obstacle of Sustainable Development. *Springer Proceedings in Business and Economics*, *1*, 395–407. https://doi.org/10.1007/978-3-031-28131-0_27

Cagigas, D., Clifton, J., Diaz-Fuentes, D., & Fernandez-Gutierrez, M. (2021). Blockchain for Public Services: A Systematic Literature Review. *IEEE Access*, *9*, 13904–13921. https://d™£oi.org/10.1109/ACCESS.2021.3052019

Dang, T. C., Van, H. V., & Van, D. Le. (2025). E-Government and Corruption in an Emerging Country: New Perspectives from a Spatiotemporal Approach. *International Review of Economics & Finance*, *100*, 104111. https://doi.org/10.1016/J.IREF.2025.104111

Data Reportal. (2025). *Digital di Seluruh Dunia*. Datareportal. Retrieved 12 April, 2025, from: https://datareportal.com/global-digital-overview

Dobrovolska, O., & Rozhkova, M. (2024). The Impact of Digital Transformation on the Anti-Corruption and Cyber-Fraud System. *Business Ethics and Leadership*, *8*(2), 231–252. https://doi.org/10.61093/bel.8(3).231-252.2024

El Kafhali, S. (2024). Blockchain-Based Electronic Voting System: Significance and Requirements. *Mathematical Problems in Engineering*, *2024*(1), 1–17. https://doi.org/10.1155/2024/5591147

Handoko, R. M., Trisna, B. A. A., Pratama, R. D., & Parhusip, J. (2024). Implementasi Blockchain untuk Keamanan Sistem Pembayaran Digital dan Optimasi Transaksi Keuangan (Studi Kasus Industri Fintech di Indonesia). *Teknik: Jurnal Ilmu Teknik dan Informatika*, *4*(2), 64–74. https://doi.org/10.51903/TEKNIK.V4I2.589

Henley & Partners. (2023). Crypto Wealth Report 2023. Henleyglobal. Retrieved 31 March, 2026, from: https://www.henleyglobal.com/publications/crypto-wealth-report/crypto-adoption-index.

Hochstetter, J., Vásquez, F., Diéguez, M., Bustamante, A., & Arango-López, J. (2023). Transparency and E-Government in Electronic Public Procurement as Sustainable Development. *Sustainability 2023, 15*(5), 4672. https://doi.org/10.3390/SU15054672

Hope, K. R. (2020). Peace, Justice and Inclusive Institutions: Overcoming Challenges to the Implementation of Sustainable Development Goal 16. *Global Change, Peace and Security*, *32*(1), 57–77. https://doi.org/10.1080/14781158.2019.1667320

Ilori, O. O., & Tanimowo, F. O. (2022). Heteroscedasticity Detection in Cross-Sectional Diabetes Pedigree Function: A Comparison of Breusch-Pagan-Godfrey, Harvey and Glejser Tests. *International Journal of Scientific and Management Research*, *05*(12), 150–163. https://doi.org/10.37502/IJSMR.2022.51211

Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023). Towards Insighting Cybersecurity for Healthcare Domains: A Comprehensive Review of Recent Practices and Trends. *Cyber Security and Applications*, *1*, 100016. https://doi.org/10.1016/J.CSA.2023.100016

Kalesnikaite, V., Neshkova, M. I., & Ganapati, S. (2023). Parsing the Impact of E-Government on Bureaucratic Corruption. *Governance*, *36*(3), 827–842. https://doi.org/10.1111/GOVE.12707

Karina, D., Oh, A., & Hamzah, Z. (2023). Unravelling Factors Shaping Purchase Intention for "Tri" Cellular Card. *International Journal of Information System and Innovation Managemen*, *1*(1), 32–45.

Katrakazas, C., Theofilatos, A., Papastefanatos, G., Härri, J., & Antoniou, C. (2020). Cyber Security and its Impact on CAV Safety: Overview, Policy Needs and Challenges. *Advances in Transport Policy and Planning*, *5*, 73–94. https://doi.org/10.1016/BS.ATPP.2020.05.001

Kim, K., & Kang, T. (2021). Will Blockchain Bring an End to Corruption?: Areas of Applications and Potential Challenges. *International Journal of Information Systems and Social Change, 10*(2), 35-44. https://doi.org/10.4018/978-1-7998-5351-0.CH100

Lee, K., Malerba, F., & Primi, A. (2020). The Fourth Industrial Revolution, Changing Global Value Chains and Industrial Upgrading in Emerging Economies. *Journal of Economic Policy Reform, 23*(4), 1-12. https://doi.org/10.1080/17487870.2020.1735386

Li, Y., & Liu, Q. (2021). A Comprehensive Review Study of Cyber-Attacks and Cyber Security; Emerging Trends and Recent Developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/J.EGYR.2021.08.126

Lykidis, I., Drosatos, G., & Rantos, K. (2021). The Use of Blockchain Technology in e-Government Services. *Computers*, *10*(12), 168. https://doi.org/10.3390/computers10120168

Malodia, S., Dhir, A., Mishra, M., & Bhatti, Z. A. (2021). Future of E-Government: An Integrated Conceptual Framework. *Technological Forecasting and Social Change*, *173*, 121102. https://doi.org/10.1016/J.TECHFORE.2021.121102

Mamulak, N. M. R., Miswadi, M., Julinaldi, J., Komarudin, R., & Syahputra, M. (2024). Blockchain Technology: Unlocking New Frontiers in Data Management and Transparency. *Global International Journal of Innovative Research*, *2*(9), 2257–2270. https://doi.org/10.59613/GLOBAL.V2I9.328

Mehawesh, S. S., & Al-Badayneh, D. M. (2025). Pakistan Journal of Life and Social Sciences Corruption Perception and Government Effectiveness in Combating Corruption, and Citizens' Satisfaction. *Pakistan Journal of Life and Social Sciences*, *23*(1), 9075-9081. https://doi.org/10.57239/PJLSS-2025-23.1.00710

Mensah, I. K. (2020). Impact of Government Capacity and E-Government Performance on the Adoption of E-Government Services. *International Journal of Public Administration*, *43*(4), 303–311. https://doi.org/10.1080/01900692.2019.1628059

Mishra, P., Pandey, C. M., Singh, U., Gupta, A., Sahu, C., & Keshri, A. (2019). Descriptive Statistics and Normality Tests for Statistical Data. *Annals of Cardiac Anaesthesia*, *22*(1), 67. https://doi.org/10.4103/ACA.ACA_157_18

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The Ethics of Algorithms: Mapping the Debate. *Big Data and Society*, *3*(2), 1-21. https://doi.org/10.1177/2053951716679679

Jafar, M. A. W. (2024). Dampak E-Government dalam Meningkatkan Efisiensi dan Efektivitas Tata Kelola Pemerintahan. *Politika Progresif : Jurnal Hukum, Politik Dan Humaniora*, *1*(4), 204–226. https://doi.org/10.62383/progres.v1i4.1303

Munari. (2024). E-Government Implementation and its Impact on Economic Efficiency Munari AMIK Tridharma Palu. *Jurnal Ekonomi*, *13*(1), 1452–1463. https://doi.org/10.54209/ekonomi.v13i01

Thanh, N. C., Huy, T. P., Pham Hong, T., & Bui Nguyen Quoc, A. (2025). Credit Risk Prediction with Corruption Perception Index: Machine Learning Approaches. *Cogent Business and Management*, *12*(1), 1-14. https://doi.org/10.1080/23311975.2025.2461731

Ningsih, D. A., Nurhasanah, & Fadillah, L. (2019). Efektivitas Pembelajaran di Luar Kelas dalam Pembentukan Sikap Percaya Diri Peserta Didik pada Mata Pelajaran IPA di Kelas V SDN 190 Cenning. *Pendidikan Dasar dan Keguruan*, *4*(2), 1–12. https://doi.org/10.47435/jpdk.v4i2.314

Nookhao, S., & Kiattisin, S. (2023). Achieving a Successful E-Government: Determinants of Behavioral Intention from Thai Citizens' Perspective. *Heliyon*, *9*(8), 18944. https://doi.org/10.1016/J.HELIYON.2023.E18944

Normand, Y. (2025). On Blockchain as a Tool Against Corporate Corruption. *Northwestern Journal of International Law & Business*, *45*(2), 235-261. https://scholarlycommons.law.northwestern.edu/njilb/vol45/iss2/3.

Nur, U., Mutiarin, D., Jovita, H. D., Palomares, P. P., & Isolana, J. B. (2025). Role of Good Governance Indicators in Controlling Corruption. *Journal of Governance and Public Policy*, *12*(1), 83–99. https://doi.org/10.18196/jgpp.v12i1.22287

Ohize, H. O., Onumanyi, A. J., Umar, B. U., Ajao, L. A., Isah, R. O., Dogo, E. M., Nuhu, B. K., Olaniyi, O. M., Ambafi, J. G., Sheidu, V. B., & Ibrahim, M. M. (2024). Blockchain for Securing Electronic Voting Systems: A Survey of Architectures, Trends, Solutions, and Challenges. *Cluster Computing*, *28*(2), 132. https://doi.org/10.1007/s10586-024-04709-8

Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in Government: Benefits and Implications of Distributed Ledger Technology for Information Sharing. *Government Information Quarterly*, *34*(3), 355–364. https://doi.org/10.1016/J.GIQ.2017.09.007

Ramadani, Ri. E., Sofyani, H., & Putra, A. Z. (2023). Faktor-Faktor yang Memengaruhi Kesiapan Pegawai Pemerintah Daerah dalam Mengadopsi Teknologi Blockchain pada Sistem Informasi Akuntansi Manajemen. *Jurnal Manajemen Dinamis*, *1*(2), 109–122. https://doi.org/10.59330/JMD.V1I2.28

Sakhnini, J., Karimipour, H., Dehghantanha, A., & Parizi, R. M. (2021). Physical Layer Attack Identification and Localization in Cyber–Physical Grid: An Ensemble Deep

Learning Based Approach. *Physical Communication*, *47*, 101394. https://doi.org/10.1016/J.PHYCOM.2021.101394

Seiam, D. A., & Salman, D. (2024). Examining the Global Influence of E-Governance on Corruption: A Panel Data Analysis. *Future Business Journal*, *10*(1), 29. https://doi.org/10.1186/s43093-024-00319-3

Senarathna, J. I. (2025). The Role of Cryptography in Blockchain: Ensuring Immutability, Transparency and Security. https://doi.org/10.20944/preprints202504.1814.v1

Sohag, K., Riad Shams, S. M., Darusalam, D., & Devalle, A. (2021). Information Digitalisation and Local Institutional Agility: Evidence from ASEAN Countries. *Technological Forecasting and Social Change*, *172*. https://doi.org/10.1016/j.techfore.2021.121063

Sriningsih, M., Hatidja, D., & Prang, J. D. (2018). Penanganan Multikolinearitas dengan Menggunakan Analisis Regresi Komponen Utama pada Kasus Impor Beras di Provinsi Sulut. *Jurnal Ilmiah Sains*, *18*(1), 18–24. https://doi.org/10.35799/jis.18.1.2018.19396

Sugiarti, R., & Akbar, L. R. (2024). The Effect of E-Government on Corruption-International Evidence. *Asia Pacific Fraud Journal*, *9*(2), 165–176. https://doi.org/10.21532/APFJOURNAL.V9I2.324

Sukarno, M., Rodriguez, M. J., & Nursamsiyah, N. (2024). E-Government Development on Control Corruption: A Lesson Learned from Singapore. *Journal of Governance and Public Policy*, *11*(3), 271–286. https://doi.org/10.18196/JGPP.V11I3.21447

Suryayusra, Anjuju, D., Ulfa, M., & Irawan, D. (2025). Analisis Keamanan Infrastruktur Teknologi Informasi dalam Menghadapi Ancaman Cybersecurity. *Journal of Data Analytics, Information, and Computer Science (JDAICS)*, *2*(1), 75–80. https://doi.org/10.70248/jdaics.v2i1.1792

Transparency International. (2023). Corruption Perceptions Index 2023. Retrieved 31 March, 2026, from: https://www.transparency.org/en/cpi/2023.

Transparency International. (2024). 2024 Corruption Perceptions Index: Corruption is Playing a Devastating Role in the Climate Crisis. Transparency International. Retrieved 31 March, 2026, from: https://www.transparency.org/en/press/2024-corruption-perceptions-index-corruption-playing-devastating-role-climate-crisis

Trequattrini, R., Palmaccio, M., Turco, M., & Manzari, A. (2024). The Contribution of Blockchain Technologies to Anti-Corruption Practices: A Systematic Literature Review. *Business Strategy and the Environment*, *33*(1), 4–18. https://doi.org/10.1002/BSE.3327

United Nations Development Programme. (1997). *Governance for Sustainable Human Development : A UNDP Policy Document*. United Nations. Retrieved 31 March, 2026, from: https://digitallibrary.un.org/record/492551?ln=en&v=pdf

Rustiarini, N. W. (2019). The Role of E-Government in Reducing Corruption: A Systematic Review. *Jurnal Perspektif Pembiayaan dan Pembangunan Daerah*, *7*(3), 269–286.

World Bank. (2023a). E-Government Development Index (EGDI). Retrieved 31 March, 2026, from: https://data360.worldbank.org/en/dataset/UN_EGDI.

World Bank. (2023b). Global Cybersecurity Index - Overall Score (ITU GCI). Worldbank. Retrieved 31 March, 2026, from: https://data360.worldbank.org/en/indicator/ITU_GCI_GCI_OVRL_SCRE?.

World Economic Forum. (2020). Blockchain Alone Can't Prevent Crime, but these 5 Use Cases Can Help Tackle Government Corruption. World Economic Forum. Retrieved 31 March, 2026, from: https://www.weforum.org/stories/2020/07/5-ways-blockchain-could-help-tackle-government-corruption/.

Zubaedah, P. A., Harliyanto, R., Situmeang, S. M. T., Siagian, D. S., & Septaria, E. (2024). The Legal Implications of Data Privacy Laws, Cybersecurity Regulations, and AI Ethics in a Digital Society. *The Journal of Academic Science*, *1*(2), 103-110. https://doi.org/10.59613/29QYPW51