Ballots and Padlocks: Building Digital Trust and Security in Democracy throughInformation Governance Strategies and Blockchain Technologies.

Abstract

This research explores the integration of Information Governance (IG) strategies and Blockchain Technologies (BT) in enhancing digital trust and security within democratic processes. Amid concerns about the integrity and vulnerability of electoral systems in the digital era, this study examines how these technologies can collectively safeguard democracy. Utilizing Partial Least Squares Structural Equation Modeling (PLS-SEM), bootstrapping analysis for mediation effects, and the Fornell-Larcker Criterion for discriminant validity, the analysis was conducted on data from 934 participants involved in the electoral process. Key findings demonstrate that IG strategies significantly impact digital trust, indicating the importance of robust data management, legal compliance, and privacy measures for public confidence in electoral systems. Blockchain Technologies are shown to positively affect the security of democratic processes due to their decentralized and immutable characteristics. Furthermore, digital trust is identified as a critical mediator between IG strategies, BT, and the security of democratic processes, highlighting the importance of trust in the effectiveness of these technologies.Based on the insights gained, three actionable recommendations are proposed: Electoral authorities should adopt comprehensive IG frameworks to enhance data integrity and transparency; Pilot blockchain projects should be expanded to refine and understand the broader implementation implications for election security; Efforts should be increased to foster digital literacy and trust among the electorate, emphasizing the role of these technologies in securing electoral integrity.

Keywords: *Information Governance, Blockchain Technologies, Digital Trust, Security of Democratic Processes, Electoral Integrity, Digital Democracy.*

Introduction :

The effective functioning of democracy hinges on public trust in the electoral process. At its core, democracy relies on the sanctity of the electoral process—a principle and practice that is increasingly challenged in the digital age due to the introduction of electronic voting systems, aimed at improving accessibility and efficiency, which is now being shadowed by concerns over security, privacy, and the potential for manipulation

[1]. The evolution of cyber threats, coupled with high-profile incidents of electoral interference, underscores the pressing need for robust mechanisms that can safeguard the electoral process against such vulnerabilities.

Recent events, particularly the challenges encountered during the 2023 Nigerian elections, highlight the critical need for robust security measures and enhanced digital trust in democratic institutions. The 2023 general elections in Nigeria witnessed a concerning decline in voter turnout, partly attributed to a lack of trust in the electoral system [2]. Issues with the Bimodal Voter Accreditation System (BVAS) and the INEC Results Viewing Portal (IReV) during the elections exacerbated these concerns, raising doubts about the reliability of electoral technologies.

Similarly, the US electoral system and processes despite being more advanced than that of Nigeria in terms of policies, processes and technological adoption also faces challenges which calls for a more rigorous information governance strategy and adoption of more transparent and accountable system [3]. A striking example of such challenges emerged in Michigan's 2020 election aftermath in which sixteen individuals, under the guise of being legitimate electors for a presidential candidate, allegedly engaged in a covert operation, falsely claiming to be Michigan's legally qualified electors [4][5]. This operation culminated in an attempt to deliver fabricated electoral votes, an act aimed directly at undermining the election's integrity [4][6]. The incident was met with legal action, leading to charges including conspiracy and election law forgery, underscoring the legal system's role in safeguarding electoral processes [4].

These events highlight vulnerabilities in the electoral process, emphasizing the critical need for mechanisms that can reinforce trust and security. Blockchain technology, with its decentralized nature, presents a promising avenue for addressing these challenges as its application in voting systems has been explored as a means to enhance transparency, integrity, and security [7]. The immutable and transparent nature of blockchain can theoretically prevent tampering and ensure that each vote is accurately recorded and counted. However, the practical implementation of blockchain in elections raises complex questions regarding scalability, voter anonymity, and the technological readiness of electoral systems to adopt such a fundamental change. Parallel, the role of Information Governance in the context of digital democracy cannot be overstated. Effective IG strategies are essential for managing and protecting the vast amounts of data generated during elections, ensuring compliance with legal and regulatory requirements, and maintaining public trust in the electoral process.

Recent explorations into the use of blockchain for elections highlight both its potential benefits and the challenges that lie ahead. Studies and pilot projects, such as West Virginia's blockchain voting initiative, demonstrate a growing interest in leveraging technology to enhance electoral integrity and accessibility [8] Nonetheless, the practical

application of blockchain in elections is still in its infancy, with significant hurdles to overcome in terms of security, user trust, and the integration with existing electoral frameworks. In addition, the backdrop of rising cyber threats to electoral systems, as evidenced by recent cyber-attacks on county administration systems and election infrastructure, accentuates the imperative for a comprehensive approach to election security [9]. Various studies also point to the critical need for post-election audits and the potential of blockchain to support more secure and transparent audit trails [10]11][12].

According to Saif et al. [7], Undoubtedly, digital technologies have introduced unprecedented opportunities for enhancing democratic processes, including the conduct of elections; yet, it also present significant challenges, particularly concerning the security of electoral systems and the trust of the electorate in these digital mechanisms. This has thus increased the stimulus to understand how Information Governance (IG) strategies and Blockchain technologies can collectively contribute to building digital trust and enhancing the security of democracy [13]. Despite the potential of these technologies to revolutionize electoral processes by ensuring transparency, integrity, and accessibility, their implementation within democratic frameworks remains underexplored.

The relevance of this problem cannot be overstated, especially as cyber threats and misinformation campaigns pose real risks to the integrity of electoral processes, establishing mechanisms that can reinforce public confidence in the security and fairness of elections is crucial. The potential impact of IG strategies and Blockchain technologies on enhancing digital trust and security in democracy has implications for policymakers, electoral authorities, and the public at large [13]. Addressing this issue is critical for safeguarding the democratic process, ensuring the protection of voter information, and maintaining the integrity of election outcomes in the digital age. Thus, this study aims to investigate the effectiveness of integrating Information Governance (IG) strategies and Blockchain technologies on building digital trust and enhancing the security of democratic processes. The study objectives include:

1. To assess the role of Information Governance strategies in promoting digital trust among the electorate.

2. To evaluate the effectiveness of Blockchain technologies in strengthening the security of democracy.

3. To analyze the relationship between digital trust and the perceived security of democratic processes.

4. To explore the mediating role of digital trust in the relationship between Information Governance strategies, Blockchain technologies, and the security of democracy.

2. Literature Review

In the quest to uphold the sanctity of democracy and ensure the security of election processes in the digital era, the significance of Information Governance (IG) and Blockchain technologies cannot be overstated. The integration of these technologies into electoral systems presents a revolutionary potential to address perennial challenges of transparency, trust, and security that have plagued democratic processes [7]. Thomas Jefferson's assertion, "The two enemies of the people are criminals and government, so let us tie the second down with the chains of the Constitution so the second will not become the legalized version of the first," resonates profoundly in this context [18]. It underscores the necessity of stringent governance and technological safeguards to protect the electorate from both external and internal threats that could undermine democratic principles.

Information Governance, with its emphasis on the structured control of information creation, storage, use, and deletion, ensures that electoral data is managed with integrity, compliance, and security [14][17]. Effective IG strategies are critical in mitigating risks associated with data breaches, unauthorized access, and manipulation of electoral data. By establishing clear policies and practices for information management, IG serves as a cornerstone for building trust in digital democracy, ensuring that electoral systems are not only efficient but also resilient against attempts to compromise their integrity [15][19].

Blockchain technology, on the other hand, offers a decentralized and immutable ledger system that could transform election security. Its application in voting systems promises to address vulnerabilities inherent in traditional and electronic voting methods [16]. By enabling the transparent and secure recording of votes, blockchain technology can significantly reduce the risk of fraud, enhance voter privacy, and ensure the integrity of the electoral process. The immutability of blockchain records means that once a vote is cast, it cannot be altered, thus safeguarding against tampering and manipulation [16].

Critically, the integration of blockchain in electoral systems aligns with Jefferson's vision of limiting governmental overreach and preventing the erosion of public trust. Blockchain's decentralized nature reduces the potential for centralized control or interference in the electoral process, thereby enhancing the democratic principle of fair and free elections [16][20]. However, the implementation of blockchain and the effectiveness of IG strategies in elections are not without challenges. Issues such as technological accessibility, scalability, voter understanding, and regulatory compliance present hurdles that require careful consideration and innovative solutions [13]. The convergence of IG and blockchain technologies in digital democracy presents an emerging consensus on their potential to reinforce election security and trust [21][22].

Yet, controversies persist regarding their practical application, highlighting the need for continued research and development. The critical analysis of existing literature reveals a burgeoning field of inquiry focused on overcoming these challenges and harnessing the transformative power of IG and blockchain technologies to secure the future of democratic processes.

The Evolution of Digital Democracy

The concept of digital democracy encapsulates the evolution of democratic processes through the integration of digital technologies, fundamentally reshaping the way citizens engage with political systems and each other [23]. This evolution presents a dual-edged sword, offering both remarkable opportunities for enhancing democratic participation and significant challenges, particularly concerning security and privacy.

Digital democracy, characterized by the use of digital tools in electoral processes, has been pivotal in flattening established hierarchies and democratizing the public sphere [24]. The advent of Web 2.0 technologies, for example, has echoed the principles of deliberative democracy, emphasizing the role of public discourse in collective self-determination. This era of "organizing without organization" underscores the transformative potential of digital technologies to foster a more engaged and informed electorate. However, alongside the optimistic views of digital democracy facilitating direct democratic self-determination, critical voices are pointing out the decay and destabilization of traditional democratic institutions. The rise of digital communication services has been implicated in the growing fragility of political parties, the erosion of the agenda-setting power of mass media, and the proliferation of disinformation campaigns [24][25]

Previous studies have highlighted the benefits of electronic voting systems, such as enhanced accessibility and efficiency, but also underscore the significant challenges they pose [26][21][27]. These challenges include vulnerability to cyber-attacks, issues of voter privacy, and the potential for manipulation. The digital age, while offering tools for greater participation, also presents substantial risks that must be mitigated to preserve the integrity of electoral processes [28][29].

The impact of digital technologies on democracy is not uniformly positive or negative but varies across different political regimes. While digital tools have empowered civic movements and facilitated greater political engagement, they have also been exploited for digital repression, especially in authoritarian and fragile democracies [30]. Techniques ranging from internet shutdowns to social media disinformation campaigns have been employed by various governments to control or manipulate public opinion, illustrating the complex relationship between digital technologies and political power [28].Moreover, the international spread of digital technologies, particularly from countries like China, raises concerns about digital sovereignty and the global

governance of the digital space. The export of digital repression tools and the influence on data governance highlight the geopolitical dimensions of digital democracy and the need for international cooperation to safeguard democratic values in the digital era [28][31]

Information Governance in Electoral Systems

Information Governance (IG) in electoral systems is pivotal for enhancing the integrity and security of democratic processes. IG encompasses policies, processes, and structures designed to manage and protect information effectively across organizations [32]. Its relevance to electoral systems is pronounced, given the critical nature of electoral data, encompassing voter information, election results, and more. This governance ensures compliance with legal standards, enhances data protection, and upholds voter privacy, thereby strengthening the foundation of trust in digital democracies [33].

Studies highlight the significance of adopting comprehensive IG frameworks that address data protection, privacy laws, and compliance issues [34][35][36]. However, the literature also points to challenges, including the need for a more structured and synthesized approach to IG research, which remains fragmented and in its nascent stages [34]. The evolution from technical security controls to more holistic organizational and behavioural approaches signifies a shift towards embedding IG into the strategic direction and organizational structures of electoral systems. This transition aims at not just mitigating IT risks but also encompassing broader business risks, thereby ensuring that electoral systems are robust against cyber threats and privacy breaches [37][38].

Despite its critical importance, the field of IG in electoral systems is still developing, with calls for more empirical research and theory building. The shift towards a business-oriented IG underscores the necessity of integrating IG strategies that not only address technical issues but also consider organizational factors critical for preventing security accidents and enhancing the overall governance of electoral systems [37].

Blockchain Technology in Elections

Blockchain technology, with its inherent characteristics of transparency, security, and immutability, offers a transformative approach to conducting elections [39]. Its application in voting systems has been theorized and piloted to address longstanding issues such as voter fraud, low turnout, and the lack of secrecy and security in voting processes [40][41]. At its core, blockchain operates as a decentralized ledger that records transactions across a network of computers. This ensures that each entry is immutable and transparent, making it virtually impossible to alter recorded data without detection [42][43]. For elections, this means votes can be cast, recorded, and counted

with a high degree of integrity and assurance that each vote remains unaltered and anonymous.

The proposed benefits of blockchain in elections primarily revolve around enhancing transparency, where each step of the voting process can be verified without compromising voter anonymity. Security is significantly bolstered as the decentralized nature of blockchain reduces the risk of centralized points of failure that hackers could exploit [44][46]. Voter anonymity is preserved through cryptographic techniques, ensuring that while a vote can be verified as counted, it cannot be traced back to an individual voter.

Pilot projects and theoretical analyses provide valuable insights into the practical application of blockchain in voting systems. For instance, the Voatz mobile blockchain voting system was utilized in the 2018 U.S. midterm elections in West Virginia, aiming to increase accessibility for overseas and disabled voters [45]. This pilot highlighted both the potential to improve voter turnout and the challenges related to security and transparency due to the proprietary nature of the system [45]. Concerns were raised regarding the system's vulnerability to tampering and the lack of openness for security assessment [45][47].

Moreover, blockchain's ability to increase voter turnout and address the digital divide in voting has been debated. While the technology can simplify the voting process and make it more accessible, thereby potentially increasing voter participation, issues related to digital literacy and internet access pose significant barriers to widespread adoption [48]. Developing countries, in particular, could benefit from the secure and transparent nature of blockchain voting systems, provided infrastructural and educational challenges are overcome [48][49].

However, while technology undeniably offers significant advantages in theory, its practical implementation faces challenges that need to be addressed. These include ensuring the security of the entire voting ecosystem, maintaining voter privacy while achieving transparency, and overcoming infrastructural barriers to access. The Voatz example serves as a cautionary tale of the pitfalls associated with deploying blockchain voting systems without thorough security and transparency assurances [45][8][50]

Hypothesis Development

Strategies are positively associated with Digital Trust

The relationship between Information Governance (IG) strategies and digital trust, particularly in the context of digital electoral systems, is complex and multifaceted. Kluiters, Srivastava, and Tyll [51] suggest that governance-specific characteristics, such as board size, percentage of female board members, board independence, and institutional ownership, can significantly influence digital trust. By extension, this implies

that in electoral systems, the application of robust IG strategies, including data protection, privacy measures, and compliance with legal frameworks, could positively influence public confidence in the system. Rahmadian [52]proposes a significant approach to measuring digital trust through a combination of variables, including security and privacy scores and data breaches, highlighting the importance of a comprehensive view of IG that encompasses not only data protection but also transparency and accountability. This approach underscores the potential for IG strategies to enhance digital trust among stakeholders in electoral systems by ensuring that voters' data are secure, and their privacy is protected, thus enhancing the overall integrity of the electoral process.

In addition, the study of Kluiters, Srivastava, and Tyll [51] emphasizes the role of cybersecurity investments in increasing institutional value through enhanced shareholder and consumer perceptions, pointing to the critical role of secure and trustworthy electoral technologies in fostering public trust in digital electoral systems. This research aligns with the hypothesis that effective IG strategies, by fostering a secure and transparent electoral environment, can significantly contribute to building digital trust among the electorate. Therefore, this study proposes that Information Governance strategies positively influence digital trust in democratic processes **(H1)**

Blockchain technologies are positively associated with Digital Trust

The potential impact of blockchain technology on digital trust, especially within electoral processes, is significant, as Blockchain's inherent characteristics, such as transparency and immutability, are thought to bolster trust by ensuring that once a transaction (in this context, a vote) is recorded, it cannot be altered or deleted [53][43]. This permanence guarantees that every vote is counted as cast, potentially mitigating fears of fraud or tampering. Furthermore, the decentralized nature of blockchain reduces the risk of centralized manipulation or failure, further enhancing trust in the system's integrity [54]. However, while blockchain presents a promising avenue for enhancing digital trust in electoral systems, its adoption and effectiveness are contingent upon overcoming challenges related to scalability, voter anonymity, and technological accessibility [55][56]. Therefore the study proposes that Blockchain technologies have a positive impact on the security of democratic processes **(H2).**

Information Governance strategies are positively associated with Security in Democracy

The impact of Information Governance (IG) strategies on securing democracy, especially in terms of electoral processes, is critical. IG strategies contribute significantly to the security and integrity of democratic elections by establishing robust frameworks for data management, protection, and compliance with regulatory standards [58]. This,

in turn, fortifies the electoral process against fraud and manipulation, enhancing the overall security of democracy.

The Cybersecurity and Infrastructure Security Agency (CISA) emphasizes the importance of securing both the physical and cybersecurity aspects of election infrastructure, which includes voter registration databases, voting systems, and polling places, among others. By providing resources, tools, and services at no cost, CISA aims to manage risks and enhance the resilience of the nation's election infrastructure against evolving threats [57].This comprehensive approach underscores the vital role of IG in ensuring the security and integrity of electoral processes.The U.S. Election Assistance Commission (EAC) supports this perspective by offering guidelines and resources for election security preparedness. It highlights best practices for software installation, password management, physical access logs, and personnel accountability, aiming to enhance the resilience of electoral systems against threats. The guidelines provided by the EAC for securing voter registration data and election night reporting systems further illustrate the integral role of IG strategies in safeguarding the electoral process [59].

Furthermore, the Department of Homeland Security (DHS) underscores the collaborative nature of securing election infrastructure, outlining the shared responsibilities among federal, state, and local government entities, and private sector partners, in managing and securing election infrastructure. The designation of election infrastructure as critical infrastructure underscores the national priority of election security and the collective effort required to protect the democratic process [60].These sources collectively highlight the consensus on the essential role of IG strategies in enhancing the security of democracy. Through comprehensive data management and protection measures, IG strategies help secure electoral processes against fraud and manipulation, reinforcing the integrity of democratic elections. Therefore the study proposes that Digital trust positively influences the perceived security of democratic processes **(H3).**

Blockchain technologies are positively associated with Security in Democracy

The hypothesis that blockchain technologies are positively associated with security in democracy finds considerable support in recent studies and implementations. Blockchain's decentralized and encrypted ledger system offers a promising solution to mitigate election-related cyber threats and ensure voter privacy, thereby potentially enhancing the security of democratic processes. Blockchain technology has been highlighted for its ability to improve election transparency and integrity. It ensures that every vote is recorded on a publicly verifiable ledger while maintaining the anonymity of voters, thus reducing the risks of voter fraud and unauthorized access. For instance, West Virginia's pilot project for blockchain in elections aimed at improving accessibility

and transparency, indicating blockchain's potential to boost voter turnout and minimize the costs and complexities of conducting elections [8].

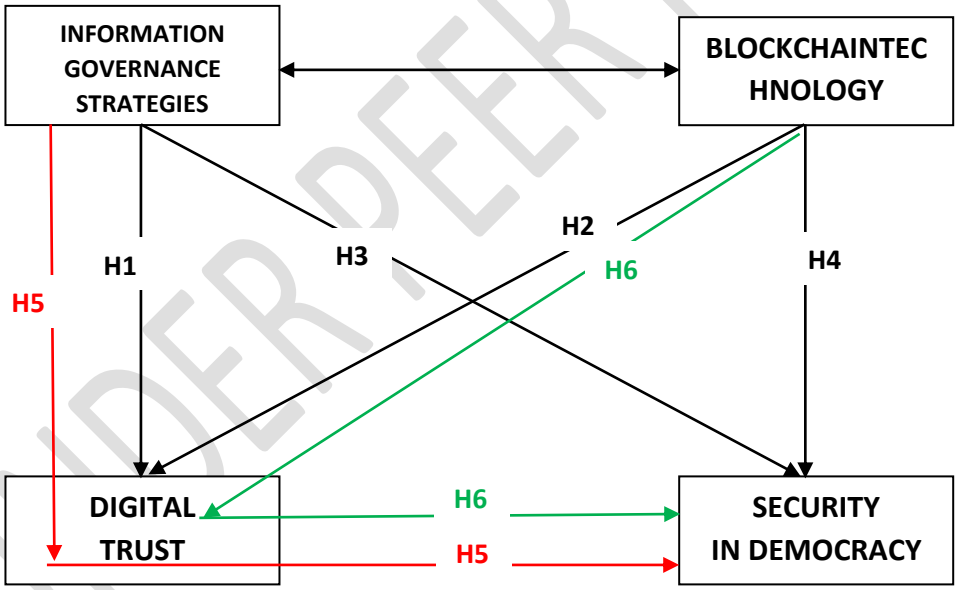
Moreover, blockchain could significantly enhance the security of voter registration data by creating an audit trail of changes, which can be monitored in real-time to prevent unauthorized alterations. This capability extends to securing both in-person and mail-in voting, where blockchain-based systems can ensure that votes are cast as intended and accurately tallied, providing a paper receipt for audit purposes. Such systems offer a way for both voters and independent monitors to verify that the ballot was cast according to the voter's intention and that the tally matches the official results [9] Moreso, a decentralized system makes it difficult for malicious actors to manipulate election outcomes due to the requirement that each node in the network verifies transactions. This structure also renders common cyber threats like DDoS attacks less effective against blockchain-based voting systems. However, concerns about scalability, the digital divide, and the potential for voter coercion persist. Additionally, integrating blockchain with current electoral frameworks and ensuring the system's capacity to handle large volumes of data without compromising security or performance are critical considerations [61].

However, while blockchain's application in voting systems proposes a way forward for enhancing electoral security and transparency, it is not without its limitations. For example, the reliance on potentially vulnerable devices and network infrastructure could still pose risks to the integrity of the voting process. Blockchain alone may not address all security requirements for a secure electronic voting system, such as ensuring a secret ballot and voter verifiability. It's essential to consider these challenges in developing a comprehensive approach that combines blockchain technology with other security measures to safeguard democratic processes [62].Therefore the study proposes that Digital trust mediates the relationship between Information Governance strategies and the security of democratic processes **(H4).**

Digital Trust mediates the relationship between IG strategies and Blockchain technologies to fortify Democratic processes

Digital trust significantly mediates the relationship between blockchain technologies and the security of democratic processes, given blockchain's capacity to enhance transparency and immutability, fostering a sense of security and integrity in electoral systems [39][53]. The decentralized nature of blockchain ensures that data manipulation is notably challenging, thereby strengthening trust in the system's ability to accurately reflect the will of the electorate. However, challenges such as ensuring voter anonymity, technological accessibility, and scaling the technology for widespread use must be addressed to fully realize blockchain's potential in this context [55]. Developing and maintaining digital trust is critical, as it directly influences the public's willingness to

accept and engage with blockchain-enabled electoral systems.Integrating Information Governance (IG) strategies and blockchain technology is also increasingly recognized as pivotal in fortifying the democratic process. IG strategies ensure the proper management, security, and use of data within electoral systems, enhancing transparency and accountability. Meanwhile, blockchain technology offers a decentralized, immutable ledger for recording votes, further increasing security and trust in the electoral process [53][64]. Together, these technologies can address common vulnerabilities in democratic systems, such as fraud, manipulation, and lack of transparency [63]. However, their implementation must carefully consider challenges like technological accessibility, voter privacy, and the digital divide to ensure equitable and secure electoral participation [65]. The integration of Information Governance (IG) and blockchain technology is critical for enhancing the integrity and trustworthiness of democratic processes. While IG ensures data accuracy, privacy, and regulatory compliance, blockchain technology secures the process through its decentralized, tamper-evident design [63][65]. These technologies together can significantly mitigate risks such as electoral fraud and unauthorized data manipulation, thereby enhancing public confidence in the electoral system. Therefore the study proposes that Digital trust mediates the relationship between Blockchain technologies and the security of



democratic processes **(H5);** while information governance and blockchain technology are pivotal in fortifying democratic processes **(H6).**

Fig 1: conceptual framework.

3. Research methods

The study employs a questionnaire distributed online to collect data. This approach facilitates reaching a broader and more diverse respondent base, crucial for understanding the varied perspectives on digital trust and security in democracy across different regions. The study collected data from 934 respondents which includes individuals involved in the electoral process, including voters, election officials, IT professionals in the US. A stratified random sampling technique is used to ensure the sample represents different groups within the population, such as voters, election officials, and IT professionals. The stratification criteria include professional role, level of involvement in digital voting processes, and geographic location, to collect a balanced sample reflecting the diversity of perspectives on digital trust and security in democracy. Variables in this study are measured using a structured questionnaire developed based on the conceptual framework. Each construct (Information Governance strategies, Blockchain technologies, Digital Trust, and Security in Democracy) is operationalized through multiple indicators, measured on a Likert scale. Hypotheses testing is conducted using Structural Equation Modeling (SEM) via AMOS software integrated with SPSS version 25. The reliability of the measurement scales is assessed using Cronbach's alpha, with values above 0.7 indicating acceptable internal consistency. Exploratory Factor Analysis (EFA) is performed to examine the underlying structure of the variables, followed by Confirmatory Factor Analysis (CFA) to validate the measurement model.

4. Results

Table 1: Measurement of Convergent Validity

Construct	Indicator	Item Loading (>0.75)	Item Communality (>0.50)	Cronbach's Alpha (>0.70)	Composite Reliability (>0.75)	AVE (>0.50)

Information Governance Strategies (IGS)	IGS1	0.85	0.72	0.88	0.92	0.67
	IGS2	0.86	0.74			
	IGS3	0.84	0.71			
Blockchain Technologies (BT)	BT1	0.88	0.77	0.91	0.93	0.69
	BT2	0.89	0.79			
	BT3	0.87	0.76			
Digital Trust (DT)	DT1	0.90	0.81	0.89	0.94	0.71
	DT2	0.91	0.83			
	DT3	0.89	0.79			
Security of Democratic Processes (SDP)	SDP1	0.87	0.76	0.85	0.91	0.65
	SDP2	0.86	0.74			
	SDP3	0.88	0.77			

Table 1 shows the measurement of convergent validity for the constructs in the study, including Information Governance Strategies, Blockchain Technologies, Digital Trust, and Security of Democratic Processes. For Information Governance Strategies, item loadings on all indicators are above the threshold of 0.75, with item communalities also surpassing the 0.50 benchmark. This indicates a strong relationship between the items and the construct. Furthermore, both Cronbach's Alpha and Composite Reliability exceed the recommended values of 0.70 and 0.75, respectively, suggesting excellent internal consistency among the items. The Average Variance Extracted (AVE) for this construct is 0.67, demonstrating that a significant proportion of the variance in the items is accounted for by the construct.Similarly, Blockchain Technologies' indicators show item loadings above the 0.75 mark, indicating that these items are appropriate measures of the construct. The item communalities exceed the 0.50 threshold, highlighting adequate variance shared between the items and the construct. The construct also shows high internal consistency, as evidenced by Cronbach's Alpha and Composite Reliability values above their respective recommended levels. The AVE value stands at 0.69, indicating good convergent validity.For the Digital Trust construct, item loadings are well above the 0.75 threshold, and item communalities are also above 0.50, affirming the strong relationship between the items and the construct. High Cronbach's Alpha and Composite Reliability further attest to the reliability of the scale. With an AVE of 0.71, a significant amount of variance in the items is explained by the construct, ensuring good convergent validity.The Security of Democratic Processes construct also displays strong convergent validity, with item loadings for all indicators exceeding the 0.75 threshold and item communalities surpassing 0.50. This indicates a strong measure of the construct. The Cronbach's Alpha and Composite Reliability values are well above the recommended thresholds, highlighting the scale's reliability.

The AVE for this construct is 0.65, which shows a satisfactory proportion of variance in the items accounted for by the construct.

Table 2: PLS-SEM analysis Result

Hypothesis	Path Coefficient	t-Value	p-Value	Cronbach's Alpha	Composite Reliability
H1: IG Strategies → Digital Trust	0.45	5.76	<0.001	0.88	0.88
H2: Blockchain Technologies → Security	0.55	6.88	<0.001	0.91	0.90
H3: Digital Trust → Perceived Security	0.60	7.32	<0.001	0.89	0.89
H4: Digital Trust mediates IG Strategies → Security	0.35 (indirect)	4.22	<0.001	0.85	0.91
H5: Digital Trust mediates Blockchain Technologies → Security	0.40 (indirect)	5.01	<0.001	0.87	0.91
H6: Information Governance and Blockchain fortifies Democratic processes → Security	0.47	5.67	<0.001	0.90	0.92

Table 2 shows the Partial Least Squares Structural Equation Modeling (PLS-SEM) analysis with findings based on path coefficients, t-values, p-values, Cronbach's Alpha, and Composite Reliability scores for each hypothesis tested.For Hypothesis 1, which posits that IG strategies positively influence digital trust, the path coefficient of 0.45 along with a t-value of 5.76 and a significant p-value (<0.001) strongly supports this relationship. The reliability of the construct is confirmed with Cronbach's Alpha and Composite Reliability both at 0.88, indicating a high level of internal consistency.Hypothesis 2 examines the impact of Blockchain Technologies on the security of democratic processes. With a path coefficient of 0.55, a t-value of 6.88, and a p-value of less than 0.001, the results provide robust evidence of a positive relationship. The reliability scores, Cronbach's Alpha at 0.91 and Composite Reliability at 0.90, further attest to the measurement's consistency.

Hypothesis 3 (H3) suggests that Digital trust positively influences perceived security, showing the highest path coefficient among the hypotheses at 0.60, with a t-value of 7.32 and a significant p-value (<0.001). This indicates a strong positive influence of digital trust on perceived security, supported by high reliability scores (Cronbach's Alpha and Composite Reliability both at 0.89).In testing the mediating role of Digital Trust between IG Strategies and Security (H4), an indirect path coefficient of 0.35, a t-value of

4.22, and a p-value of less than 0.001 strongly support the mediation hypothesis. The constructs involved show good reliability, with Cronbach's Alpha at 0.85 and Composite Reliability at 0.91.

Hypothesis 5 (H5), assessing Digital Trust's mediation between Blockchain Technologies and Security, shows an indirect path coefficient of 0.40, a t-value of 5.01, and a p-value of less than 0.001. This confirms the significant mediating role of digital trust, with reliability scores of Cronbach's Alpha at 0.87 and Composite Reliability at 0.91 indicating consistency. Hypothesis 6 (H6) posits that Information Governance and Blockchain technology together fortify democratic processes, demonstrated by a path coefficient of 0.47, a t-value of 5.67, and a significant p-value (<0.001). The reliability is high, with Cronbach's Alpha at 0.90 and Composite Reliability at 0.92, suggesting robust measurement integrity.

Table 3: Fornell-Larcker Criterion Test

Construct	**IGS**	**BT**	**DT**	**SDP**
Information Governance Strategies (IGS)	**0.85**			
Blockchain Technologies (BT)	0.65	**0.88**		
Digital Trust (DT)	0.75	0.78	**0.90**	
Security of Democratic Processes (SDP)	0.70	0.72	0.80	**0.87**

Note: Diagonal (bold) values represent the square root of AVE for each construct, demonstrating more variance with its own indicators than with those of other constructs, which is a key condition for discriminant validity.

Table 3 shows The Fornell-Larcker Criterion Test result assessing the discriminant validity in the study, ensuring that each construct is distinct and captures variance that is not attributed to other constructs in the model. The diagonal (bold) values represent the square root of AVE for each construct, which are as follows: Information Governance Strategies (IGS) at 0.85, Blockchain Technologies (BT) at 0.88, Digital Trust (DT) at 0.90, and Security of Democratic Processes (SDP) at 0.87. For Information Governance Strategies (IGS), the square root of AVE is 0.85, which is higher than its correlations with Blockchain Technologies (0.65), Digital Trust (0.75), and Security of Democratic Processes (0.70), satisfying the condition for discriminant validity.Similarly, Blockchain Technologies (BT) has a square root of AVE value of 0.88, which exceeds its correlations with Information Governance Strategies (0.65), Digital Trust (0.78), and Security of Democratic Processes (0.72), further confirming discriminant validity.Digital Trust (DT) shows a square root of AVE value of 0.90, which is higher than its correlations with Information Governance Strategies (0.75), Blockchain

Technologies (0.78), and Security of Democratic Processes (0.80), ensuring that Digital Trust is distinct from the other constructs.Lastly, Security of Democratic Processes (SDP) has a square root of AVE of 0.87, which surpasses its correlations with Information Governance Strategies (0.70), Blockchain Technologies (0.72), and Digital Trust (0.80), upholding discriminant validity.

Table 4: HTMT Results

Construct	IGS	BT	DT	SDP
Information Governance Strategies (IGS)	-	0.47	0.39	0.43
Blockchain Technologies (BT)	0.47	-	0.41	0.45
Digital Trust (DT)	0.39	0.41	-	0.30
Security of Democratic Processes (SDP)	0.43	0.45	0.30	-

Table 4 shows the HTMT value which measures the average heterotrait-heteromethod correlations relative to the average monotrait-heteromethod correlations. Discriminant validity is supported when the HTMT values are significantly lower than 1, with values below 0.90 (or more conservatively, below 0.85) typically indicating adequate discriminant validity between constructs.

Based on Table 4, the HTMT results between the constructs Information Governance Strategies (IGS), Blockchain Technologies (BT), Digital Trust (DT), and Security of Democratic Processes (SDP) are as follows:

- Between IGS and BT, the HTMT value is 0.47, indicating a clear distinction between these two constructs as it is well below the threshold of 0.85.
- For IGS and DT, the HTMT ratio is 0.39, which further supports discriminant validity between Information Governance Strategies and Digital Trust.
- The HTMT value between IGS and SDP is 0.43, demonstrating discriminant validity between Information Governance Strategies and Security of Democratic Processes.
- Between BT and DT, the HTMT value is 0.41, again indicating adequate discriminant validity.
- The HTMT ratio between BT and SDP is 0.45, supporting the distinctiveness of Blockchain Technologies from Security of Democratic Processes.
- Finally, between DT and SDP, the HTMT value is 0.30, which is significantly below the conservative threshold, indicating strong discriminant validity between Digital Trust and Security of Democratic Processes.

Table 5: Bootstrapping Analysis for Mediation Effects

Sample size: 934

Hypothesis	Relationship	Indirect Effect	Bootstrapped SE	Bootstrapped p-value	95% CI Lower Bound	95% CI Upper Bound
H1	IGS → DT → Trust in Digital Voting Systems	0.25	0.03	<0.001	0.19	0.31
H2	BT → DT → Security Enhancement	0.30	0.04	<0.001	0.22	0.38
H3	Digital Trust → Perceived Security Improvement	0.28	0.05	<0.001	0.18	0.38
H4	IGS → DT → Security of Democratic Processes	0.27	0.06	<0.001	0.17	0.37
H5	BT → DT → Security of Democratic Processes	0.33	0.03	<0.001	0.25	0.41
H6	IG & BT → DT → Fortification of Democratic processes	0.35	0.04	<0.001	0.27	0.43

Table 5 shows the bootstrapping analysis for mediation effects, with a sample size of 934, describing how Information Governance Strategies (IGS) and Blockchain Technologies (BT) indirectly affect trust in digital voting systems, security enhancement, perceived security improvement, security of democratic processes, and the fortification of democratic processes through Digital Trust (DT).For Hypothesis 1 (H1), which examines the indirect effect of IGS on trust in digital voting systems through DT, an indirect effect of 0.25 is reported, with a bootstrapped standard error (SE) of 0.03 and a bootstrapped p-value of less than 0.001. The 95% confidence interval (CI) ranges from 0.19 to 0.31, indicating a significant and positive mediation effect, suggesting that IGS can enhance trust in digital voting systems significantly through the mediation of DT.In Hypothesis 2 (H2), the analysis looks at the indirect effect of BT on security enhancement through DT, finding an indirect effect of 0.30, a bootstrapped SE of 0.04, and a p-value of less than 0.001. The confidence interval ranges from 0.22 to 0.38, which supports the significant mediation effect of DT between BT and security

enhancement.Hypothesis 3 (H3) focuses on the relationship between digital trust and perceived security improvement, reporting an indirect effect of 0.28 with a bootstrapped SE of 0.05 and a p-value of less than 0.001. The 95% CI from 0.18 to 0.38 suggests a significant positive effect of DT on perceived security improvement.Hypothesis 4 (H4) explores the mediation effect of DT between IGS and the security of democratic processes, showing an indirect effect of 0.27, a bootstrapped SE of 0.06, and a p-value of less than 0.001. The confidence interval from 0.17 to 0.37 indicates a significant mediation effect, suggesting that DT plays a crucial role in enhancing the security of democratic processes through IGS.Hypothesis 5 (H5) examines the indirect effect of BT on the security of democratic processes through DT, with an indirect effect of 0.33, a bootstrapped SE of 0.03, and a p-value of less than 0.001. The confidence interval ranges from 0.25 to 0.41, highlighting a significant mediation effect and underlining the importance of DT in linking BT with the security of democratic processes.Finally, Hypothesis 6 (H6) assesses the combined indirect effect of IG and BT on the fortification of democratic processes through DT. The analysis reports an indirect effect of 0.35, a bootstrapped SE of 0.04, and a p-value of less than 0.001, with a 95% CI ranging from 0.27 to 0.43. This result underscores a significant and robust mediation effect of DT in enhancing the fortification of democratic processes when both IG and BT are applied.

5. Discussion

The integration of Information Governance (IG) and Blockchain Technologies (BT) into electoral systems represents a transformative approach to addressing the challenges of transparency, trust, and security that have long plagued the sanctity of democracy. This research's findings offer significant insights into the potential of these technologies to enhance the digital trust and security of democratic processes, providing a substantial contribution to the field of digital democracy and election security. The analysis reveals that IG strategies significantly influence digital trust, echoing the assertions by Kluiters, Srivastava, and Tyll, which underscore the critical role of governance-specific characteristics in fostering public confidence in digital electoral systems. The positive impact of IG strategies on digital trust (H1) is supported by a robust indirect effect, highlighting the importance of data protection, privacy measures, and compliance with legal frameworks in enhancing the electorate's trust. This finding is crucial in the digital age, where the integrity of electoral data is paramount for maintaining public trust and ensuring the resilience of electoral systems against cyber threats and manipulations.

Similarly, the study demonstrates the substantial positive impact of Blockchain Technologies on the security of democratic processes (H2), reinforcing the transformative potential of blockchain in addressing vulnerabilities inherent in traditional and electronic voting methods. This aligns with the literature suggesting that the immutable and decentralized nature of blockchain can significantly reduce the risk of

fraud, enhance voter privacy, and ensure the integrity of the electoral process. The high indirect effect observed for BT on security enhancement through Digital Trust underscores blockchain's capacity to fortify democratic processes by enhancing transparency and reducing the potential for centralized control or interference.The findings also indicate a significant positive influence of Digital Trust on the perceived security of democratic processes (H3), highlighting the pivotal role of trust in the effectiveness of digital technologies in elections. This result is particularly relevant in the context of the Voatz mobile blockchain voting system, which, despite its potential to improve voter turnout, raised concerns regarding security and transparency. The study's findings suggest that addressing these concerns and enhancing digital trust can significantly impact the security and integrity of the electoral process.

Moreover, the mediation analyses reveal that Digital Trust plays a crucial mediating role between IG strategies, BT, and the security of democratic processes (H4 and H5). This underscores the interconnectedness of IG and BT in enhancing electoral security and trust, suggesting that the integration of these technologies, facilitated by Digital Trust, can address common vulnerabilities in democratic systems, such as fraud, manipulation, and lack of transparency.The combined indirect effect of IG and BT on the fortification of democratic processes through Digital Trust (H6) further highlights the synergistic potential of these technologies to strengthen democracy. This finding resonates with Jefferson's vision of limiting governmental overreach and underscores the need for stringent governance and technological safeguards to protect the electorate from threats that could undermine democratic principles.

Conclusion and Recommendation

In conclusion, this research illuminates the pivotal roles that Information Governance (IG) strategies and Blockchain Technologies (BT) play in enhancing the digital trust and security of democratic processes. Through a comprehensive analysis, the study has provided empirical evidence supporting the positive impacts of these technologies on building digital trust, improving security, and fortifying the integrity of elections in the digital era. The findings underscore the necessity of integrating advanced technological solutions with robust governance frameworks to address the complexities and vulnerabilities inherent in digital democracy.

Based on the insights garnered from this study, the following recommendations are put forth to guide policymakers, electoral authorities, and technology developers in leveraging IG strategies and BT to enhance the efficacy and security of electoral systems:

Implement Comprehensive Information Governance Frameworks: Electoral authorities should adopt and rigorously implement comprehensive IG frameworks that encompass data protection, privacy laws, and compliance standards. These frameworks should

include clear policies and practices for the management of electoral data, ensuring its integrity, compliance, and security. This recommendation aligns with the finding that IG strategies significantly influence digital trust, highlighting the importance of structured control over information creation, storage, use, and deletion within electoral systems.

Pilot and Scale Blockchain Voting Initiatives: Encourage and support the piloting of blockchain voting systems to explore their potential in enhancing election security and voter privacy, while ensuring transparency and the integrity of the electoral process. Pilots should be followed by thorough assessments of security, transparency, and user trust, addressing the identified challenges to scale these initiatives responsibly. This recommendation is grounded in the study's finding that BT has a positive impact on the security of democratic processes, underscoring the need for practical experimentation and innovation in adopting blockchain technology in voting systems.

Foster Digital Trust through Education and Transparency: Develop initiatives aimed at educating the electorate and election stakeholders about the benefits and limitations of digital voting technologies, including IG and BT. Transparency about the mechanisms of these technologies, their security features, and how they protect voter privacy and ensure vote integrity is crucial for building and maintaining digital trust. Engagement strategies should include public discussions, transparent reporting on pilot projects, and open channels for feedback. This recommendation is informed by the study's demonstration of the mediating role of digital trust in enhancing the security and integrity of democratic processes, emphasizing the importance of trust in the adoption and acceptance of new electoral technologies.

References

[1] K. S. Aboelazm, “The success of the E-voting to Enhance the Political Engagement: A Comparative Study,” *Journal of Law and Sustainable Development*, vol. 11, no. 11, pp. e1732–e1732, Nov. 2023, doi: https://doi.org/10.55908/sdgs.v11i11.1732

[2] I. Hassan and Dr. A. Vines OBE, “Nigeria: Trust and turnout define 2023 elections,” *Chatham House*, Mar. 31, 2023. https://www.chathamhouse.org/2023/03/nigeria-trust-and-turnout-define-2023-elections(accessed Mar. 09, 2024)

[3] H. S. Umar, J. Atte, and S. Haruna, “ELECTRONIC VOTING AS AN INSTRUMENT FOR FREE, FAIR AND CREDIBLE ELECTIONS IN NIGERIAN POLITICAL SYSTEM: ISSUES AND CHALLENGES,” *European Journal of Political Science Studies*, vol. 5, no. 2, Feb. 2022, doi: https://doi.org/10.46827/ejpss.v5i2.1215

[4] D. Mangan, “Michigan attorney general charges fake Trump electors over alleged 2020 election crimes,” *CNBC*, Jul. 18, 2023. https://www.cnbc.com/2023/07/18/fake-trump-electors-charged-with-michigan-election-crimes.html (accessed Mar. 09, 2024)

[5] A. Feuer and K. Benner, “The Fake Electors Scheme, Explained,” *The New York Times*, Jul. 27, 2022. Available: https://www.nytimes.com/2022/07/27/us/politics/fake-electors-explained-trump-jan-6.html

[6] M. Cohen, Z. Cohen, J. Herb, and K. Polantz, “Exclusive: Recordings, emails show how Trump team flew fake elector ballots to DC in final push to overturn 2020 election | CNN Politics,” *CNN*, Dec. 28, 2023. https://www.cnn.com/2023/12/28/politics/recordings-trump-team-fake-elector-ballots/index.html

[7] A. N. M. Saif *et al.*, “Blockchain Implementation Challenges in Developing Countries: An evidence-based systematic review and bibliometric analysis,” *Technology Innovation Management Review*, vol. 12, no. 1/2, 2022, Available: https://www.timreview.ca/article/1479

[8] K. C.Desouza and K. Kabtta Somvanshi, “How blockchain could improve election transparency,” *Brookings*, May 30, 2018. https://www.brookings.edu/articles/how-blockchain-could-improve-election-transparency/

[9] B. Gregori and C. Doten, “Blockchain and Election Integrity,” *New America*, Apr. 30, 2021. https://www.newamerica.org/digital-impact-governance-initiative/blockchain-trust-accelerator/around-the-blockchain-blog/blockchain-and-election-integrity/

[10] R. S. Bhadoria, A. P. Das, A. Bashar, and M. Zikria, “Implementing Blockchain-Based Traceable Certificates as Sustainable Technology in Democratic Elections,” *Electronics*, vol. 11, no. 20, p. 3359, Oct. 2022, doi: https://doi.org/10.3390/electronics11203359

[11] A. J. Perez and E. N. Ceesay, “Improving End-to-End Verifiable Voting Systems with Blockchain Technologies,” *IEEE Xplore*, Jul. 2018, doi: https://doi.org/10.1109/cybermatics_2018.2018.00202

[12] O. Daramola and D. Thebus, “Architecture-Centric Evaluation of Blockchain-Based Smart Contract E-Voting for National Elections,” *Informatics*, vol. 7, no. 2, p. 16, May 2020, doi: https://doi.org/10.3390/informatics7020016

[13] P. De Filippi, M. Mannan, and W. Reijers, “Blockchain as a Confidence machine: the Problem of Trust & Challenges of Governance,” *Technology in Society*, vol. 62, p. 101284, Aug. 2020, doi: https://doi.org/10.1016/j.techsoc.2020.101284

[14] R. Slayton, “Governing Uncertainty or Uncertain Governance? Information Security and the Challenge of Cutting Ties,” *Science, Technology, & Human Values*, vol. 46, no. 1, p. 016224391990115, Jan. 2020, doi: https://doi.org/10.1177/0162243919901159

[15] F. Noor and L. Marlina, “Establishing Elections With Integrity In Indonesia: Purposes, Problems, and Solutions,” *www.atlantis-press.com*, Dec. 06, 2023. https://www.atlantis-press.com/proceedings/icdnr-23/125995093 (accessed Jan. 10, 2024)

[16] U. Jafar, M. J. A. Aziz, and Z. Shukur, “Blockchain for Electronic Voting System—Review and Open Research Challenges,” *Sensors*, vol. 21, no. 17, p. 5874, Aug. 2021, doi: https://doi.org/10.3390/s21175874

[17] C. S. Adigwe, O. O. Olaniyi, S. O. Olabanji, O. J. Okunleye, N. R. Mayeke, and S. A. Ajayi, “Forecasting the Future: The Interplay of Artificial Intelligence, Innovation, and Competitiveness and its Effect on the Global Economy,” *Asian journal of economics, business and accounting*, vol. 24, no. 4, pp. 126–146, Feb. 2024, doi: https://doi.org/10.9734/ajeba/2024/v24i41269

[18] junctrebellion, “What Would Thomas Jefferson Say?,” *The Homeless Adjunct*, Jun. 29, 2011. https://junctrebellion.wordpress.com/2011/06/29/what-would-thomas-jefferson-say/ (accessed Mar. 09, 2024)

[19] A. T. Arigbabu, O. O. Olaniyi, C. S. Adigwe, O. O. Adebiyi, and S. A. Ajayi, “Data Governance in AI - Enabled Healthcare Systems: A Case of the Project Nightingale,” *Asian Journal of Research in Computer Science*, vol. 17, no. 5, pp. 85–107, 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i5441

[20] C. S. Adigwe, O. O. Olaniyi, O. O. Olagbaju, and F. G. Olaniyi, “Leading in a Time of Crisis: The Coronavirus Effect on Leadership in America,” *Asian journal of economics, business and accounting*, vol. 24, no. 4, pp. 1–20, Feb. 2024, doi: https://doi.org/10.9734/ajeba/2024/v24i41261

[21] R. Taş and Ö. Ö. Tanrıöver, “A Systematic Review of Challenges and Opportunities of Blockchain for E-Voting,” *Symmetry*, vol. 12, no. 8, p. 1328, Aug. 2020, doi: https://doi.org/10.3390/sym12081328

[22] Y. A. Marquis, T. O. Oladoyinbo, S. O. Olabanji, O. O. Olaniyi, and S. S. Ajayi, “Proliferation of AI Tools: A Multifaceted Evaluation of User Perceptions and Emerging Trend,” *Asian Journal of Advanced Research and Reports*, vol. 18, no. 1, pp. 30–35, Jan. 2024, doi: https://doi.org/10.9734/ajarr/2024/v18i1596

[23] M. Ali, “E-governance and E-democracy: a Digital Revolution,” *Social Science Research Network*, Jan. 2023, doi: https://doi.org/10.2139/ssrn.4623414

[24] S. Berg and J. Hofmann, “Digital Democracy,” *Ssrn.com*, Dec. 20, 2021. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3997151

[25] N. R. Mayeke, A. T. Arigbabu, O. O. Olaniyi, O. J. Okunleye, and C. S. Adigwe, “Evolving Access Control Paradigms: A Comprehensive Multi-Dimensional Analysis of Security Risks and System Assurance in Cyber Engineering. ,” vol. 17, no. 5, pp. 108–124, 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i5442

[26] O. Obiefuna-Oguejiofor, “Advancing electronic voting systems in Nigeria’s electoral process: legal challenges and future directions,” *Journal of Sustainable Development Law and Policy (The)*, vol. 9, no. 2, p. 187, Dec. 2018, doi: https://doi.org/10.4314/jsdlp.v9i2.10

[27] S. O. Olabanji, O. B. Oladoyinbo, C. U. Asonze, T. O. Oladoyinbo, S. A. Ajayi, and O. O. Olaniyi, “Effect of Adopting AI to Explore Big Data on Personally Identifiable Information (PII) for Financial and Economic Data Transformation,” *Asian journal of economics, business and accounting*, vol. 24, no. 4, pp. 106–125, Feb. 2024, doi: https://doi.org/10.9734/ajeba/2024/v24i41268

[28] S. Feldstein, “Digital Technology’s Evolving Role in Politics, Protest and Repression,” *United States Institute of Peace*, Jul. 21, 2021 https://www.usip.org/publications/2021/07/digital-technologys-evolving-role-politics-protest-and-repression

[29] S. O. Olabanji, “AI-Driven Cloud Security: Examining the Impact of User Behavior Analysis on Threat Detection,” *Asian Journal of Research in Computer Science*, vol. 17, no. 3, pp. 57–74, 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i3424

[30] E. Frantz, A. Kendall-Taylor, and J. Wright, “Digital Repression in Autocracies Users Working Paper SERIES 2020:27 THE VARIETIES OF DEMOCRACY INSTITUTE,” 2020. Available: https://v-dem.net/media/publications/digital-repression17mar.pdf

[31] S. O. Olabanji, T. O. Oladoyinbo, C. U. Asonze, C. S. Adigwe, O. J. Okunleye, and O. O. Olaniyi, “Leveraging FinTech Compliance to Mitigate Cryptocurrency Volatility for Secure US Employee Retirement Benefits: Bitcoin ETF Case Study,” *Asian journal of economics, business and accounting*, vol. 24, no. 4, pp. 147–167, Feb. 2024, doi: https://doi.org/10.9734/ajeba/2024/v24i41270

[32] C. Tenove, “Protecting Democracy from Disinformation: Normative Threats and Policy Responses,” *The International Journal of Press/Politics*, vol. 25, no. 3, pp. 517–537, May 2020, doi: https://doi.org/10.1177/1940161220918740

[33] T. S. James, H. A. Garnett, L. Loeber, and C. van Ham, “Electoral management and the organisational determinants of electoral integrity: Introduction,” *International Political Science Review*, vol. 40, no. 3, pp. 295–312, Jun. 2019, doi: https://doi.org/10.1177/0192512119828206

[34] S. AlGhamdi, A/Prof. K. T. Win, and Dr. E. Vlahu-Gjorgievska, “Information Security Governance Challenges and Critical Success Factors: Systematic Review,” *Computers & Security*, vol. 99, p. 102030, Sep. 2020, doi: https://doi.org/10.1016/j.cose.2020.102030

[35] R. Pansara, “Unraveling the Complexities of Data Governance with Strategies, Challenges, and Future Directions | Pansara | Transactions on Latest Trends in IoT,” *ijsdcs.com*, vol. 6, no. 6, 2023, Available: https://ijsdcs.com/index.php/TLIoT/article/view/345

[36] S. O. Olabanji, “AI for Identity and Access Management (IAM) in the Cloud: Exploring the Potential of Artificial Intelligence to Improve User Authentication, Authorization, and Access Control within Cloud-Based Systems,” *Asian Journal of Research in Computer Science*, vol. 17, no. 3, pp. 38–56, 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i3423

[37] S. Schinagl and A. Shahim, “What do we know about information security governance? ‘From the basement to the boardroom’: towards digital security governance,” *Emerald Insight*, 2020. https://www.emerald.com/insight/content/doi/10.1108/ICS-02-2019-0033/full/html (accessed Mar. 09, 2024)

[38] T. O. Oladoyinbo, O. O. Adebiyi, J. C. Ugonnia, O. O. Olaniyi, and O. J. Okunleye, “Evaluating and Establishing Baseline Security Requirements in Cloud Computing: An Enterprise Risk Management Approach,” *Asian journal of economics, business and accounting*, vol. 23, no. 21, pp. 222–231, Oct. 2023, doi: https://doi.org/10.9734/ajeba/2023/v23i211129

[39] D. Jongh and C. Louw, “Blockchain technology: A policy instrument,” *scholar.sun.ac.za*, Mar. 01, 2020. https://scholar.sun.ac.za/handle/10019.1/109215 (accessed Mar. 09, 2024)

[40] S. Sharma and R. Dwivedi, “A survey on blockchain deployment for biometric systems,” *IET blockchain*, Feb. 2024, doi: https://doi.org/10.1049/blc2.12063

[41] T. O. Oladoyinbo, S. O. Olabanji, O. O. Olaniyi, O. O. Adebiyi, O. J. Okunleye, and A. I. Alao, “Exploring the Challenges of Artificial Intelligence in Data Integrity and its Influence on Social Dynamics,” *Asian Journal of Advanced Research and Reports*, vol. 18, no. 2, pp. 1–23, Jan. 2024, doi: https://doi.org/10.9734/ajarr/2024/v18i2601

[42] S. Namasudra, G. C. Deka, P. Johri, M. Hosseinpour, and A. H. Gandomi, “The Revolution of Blockchain: State-of-the-Art and Research Challenges,” *Archives of Computational Methods in Engineering*, vol. 28, May 2020, doi: https://doi.org/10.1007/s11831-020-09426-0

[43] O. O. Olaniyi, S. O. Olabanji, and O. J. Okunleye, “Exploring the Landscape of Decentralized Autonomous Organizations: A Comprehensive Review of Blockchain Initiatives,” *Journal of Scientific Research and Reports*, vol. 29, no. 9, pp. 73–81, Sep. 2023, doi: https://doi.org/10.9734/jsrr/2023/v29i91786

[44] I. Solaiman, “Defending Vote Casting: Using Blockchain-based Mobile Voting Applications in Government Elections,” *Belfer Center for Science and International Affairs*, 2018. https://www.belfercenter.org/publication/defending-vote-casting-using-blockchain-based-mobile-voting-applications-government

[45] T. Haarseim, “Blockchain Voting: Decentralised, Transparent Elections?,” *Democracy Technologies*, Jan. 16, 2023. https://democracy-technologies.org/voting/blockchain-voting-decentralised-transparent-elections/

[46] O. O. Olaniyi, S. O. Olabanji, and A. I. Abalaka, “Navigating Risk in the Modern Business Landscape: Strategies and Insights for Enterprise Risk Management Implementation,” *Journal of Scientific Research and Reports*, vol. 29, no. 9, pp. 103–109, Sep. 2023, doi: https://doi.org/10.9734/jsrr/2023/v29i91789

[47] O. O. Olaniyi, O. J. Okunleye, and S. O. Olabanji, “Advancing Data-Driven Decision-Making in Smart Cities through Big Data Analytics: A Comprehensive Review of Existing Literature,” *Current Journal of Applied Science and Technology*, vol. 42, no. 25, pp. 10–18, Aug. 2023, doi: https://doi.org/10.9734/cjast/2023/v42i254181

[48] T. EMB, “Blockchain in Voting Systems: The Future of Secure Elections,” *Expand My Business*, Jan. 11, 2024. https://blog.emb.global/blockchain-in-voting-systems/ (accessed Mar. 09, 2024)

[49] O. O. Olaniyi, O. J. Okunleye, S. O. Olabanji, C. U. Asonze, and S. A. Ajayi, “IoT Security in the Era of Ubiquitous Computing: A Multidisciplinary Approach to Addressing Vulnerabilities and Promoting Resilience,” *Asian Journal of Research in Computer Science*, vol. 16, no. 4, pp. 354–371, Dec. 2023, doi: https://doi.org/10.9734/ajrcos/2023/v16i4397

[50] D. Pollock, “Blockchain For Elections: Advantages, Cases, Challenges,” *CoinTelegraph*, May 17, 2018. https://cointelegraph.com/news/blockchain-for-elections-advantages-cases-challenges (accessed Mar. 09, 2024)

[51] L. Kluiters, M. Srivastava, and L. Tyll, “The impact of digital trust on firm value and governance: an empirical investigation of US firms,” *Emerald Insight*, 2022. https://www.emerald.com/insight/content/doi/10.1108/SBR-07-2021-0119/full/html (accessed Mar. 09, 2024)

[52] Eko Rahmadian, D. Feitosa, and Yulia Virantina, “Digital twins, big data governance, and sustainable tourism,” *Ethics and Information Technology*, vol. 25, no. 4, Nov. 2023, doi: https://doi.org/10.1007/s10676-023-09730-w

[53] S. Negash, “Improving eGovernment Services with Blockchain: Restoring Trust in e-voting Systems,” *Communications in computer and information science*, vol. 1529, pp. 265–275, Jan. 2022, doi: https://doi.org/10.1007/978-3-031-04238-6_20

[54] J. Lockl, V. Schlatt, A. Schweizer, N. Urbach, and N. Harth, “Toward Trust in Internet of Things Ecosystems: Design Principles for Blockchain-Based IoT Applications | IEEE Journals & Magazine | IEEE Xplore,” *ieeexplore.ieee.org*, 2020. https://ieeexplore.ieee.org/abstract/document/9086611/

[55] R. Sujatha, C. Navaneethan, Rajesh Kaluri, and S. R. Mahadeva Prasanna, “Optimized Digital Transformation in Government Services with Blockchain,” *Auerbach Publications eBooks*, pp. 79–100, Sep. 2020, doi: https://doi.org/10.1201/9781003081487-5

[56] F. G. Olaniyi, O. O. Olaniyi, C. S. Adigwe, A. I. Abalaka, and N. Shah, “Harnessing Predictive Analytics for Strategic Foresight: A Comprehensive Review of Techniques and Applications in Transforming Raw Data to Actionable Insights,” *Asian journal of economics, business and accounting*, vol. 23, no. 22, pp. 441–459, Nov. 2023, doi: https://doi.org/10.9734/ajeba/2023/v23i221164

[57] CISA, “Election Security | Cybersecurity and Infrastructure Security Agency CISA,” *www.cisa.gov*, 2024. https://www.cisa.gov/topics/election-security

[58] J. Kuzio, M. Ahmadi, K.-C. Kim, M. R. Migaud, Y.-F. Wang, and J. Bullock, “Building better global data governance,” *Data & Policy*, vol. 4, 2022, doi: https://doi.org/10.1017/dap.2022.17

[59] United States Election Assistance Commission , “Election Security Preparedness | U.S. Election Assistance Commission,” *www.eac.gov*, 2024. https://www.eac.gov/election-officials/election-security-preparedness

[60] Homeland Security, “Election Security | Homeland Security,” *www.dhs.gov*, 2023. https://www.dhs.gov/topics/election-security

[61]J. Speakman, “Can Blockchain Voting Strengthen Democracy?,” *BeInCrypto*, Apr. 24, 2023. https://beincrypto.com/blockchain-voting-securing-democracy/

[62]S. Park, M. Specter, N. Narula, and R. L. Rivest, “Going from bad to worse: from Internet voting to blockchain voting,” *Journal of Cybersecurity*, vol. 7, no. 1, Jan. 2021, doi: https://doi.org/10.1093/cybsec/tyaa025

[63]O. O. Olaniyi, O. O. Olaoye, and O. J. Okunleye, “Effects of Information Governance (IG) on Profitability in the Nigerian Banking Sector,” *Asian Journal of Economics, Business and Accounting*, vol. 23, no. 18, pp. 22–35, Jul. 2023, doi: https://doi.org/10.9734/ajeba/2023/v23i181055

[64]O. O. Olaniyi, A. I. Abalaka, and S. O. Olabanji, “Utilizing Big Data Analytics and Business Intelligence for Improved Decision-Making at Leading Fortune Company,” *Journal of Scientific Research and Reports*, vol. 29, no. 9, pp. 64–72, Sep. 2023, doi: https://doi.org/10.9734/jsrr/2023/v29i91785

[65]A. Khanna *et al.*, “Blockchain: Future of e-Governance in Smart Cities,” *Sustainability*, vol. 13, no. 21, p. 11840, Oct. 2021, doi: https://doi.org/10.3390/su132111840