PILAR Nusa Mandiri: Journal of Computing and Information System
Vol. 22, No. 1 March 2026 | DOI: 10.33480/pilar.v22i1.8254

BALANCING SECRECY AND TRANSPARENCY IN SMART CITIES: A SYSTEMATIC REVIEW OF BLOCKCHAIN-BASED GOVERNMENT DATA MANAGEMENT

Nabil Abdallh Abbas Almotawkel*; Abdulrahman Mohammed Hussein Obaid

Faculty of Engineering and Computer Sciences
21 September University for Medical and Applied Sciences, Sana'a, Yemen
https://21umas.edu.ye/
dr.almotawkel@21umas.edu.ye*, dr.obaid@21umas.edu.ye
(*) Corresponding Author

Abstract—*Blockchain offers a promising solution to recurring problems in centralized government data systems, including security vulnerabilities, inefficiencies, and declining public trust. Blockchain's decentralized and tamper-resistant architecture provides a mechanism to balance transparency and confidentiality in the management of public data. This paper presents a systematic review of the application of blockchain technology in the government domain, evaluating its impact on data security, efficiency, and public participation. This systematic review was conducted following the PRISMA protocol and searched the Scopus database for publications from 2016 to 2025. Of the 592 publications retrieved, 49 met the eligibility and quality criteria. A thematic synthesis was conducted on the results with respect to transparency, confidentiality, governance, and scalability. The findings indicate that blockchain has the potential to enhance transparency and data security through the creation of tamper-resistant records that strengthen public oversight. Blockchain also has the potential to improve the efficiency of public service delivery through digital platforms such as land registry systems and health record management. However, challenges remain, particularly related to scalability and regulatory frameworks for the adoption and implementation of the technology. Therefore, adaptive regulatory frameworks and appropriate governance mechanisms are required to support fair and sustainable adoption of blockchain technology in government data management.*

Keywords: *blockchain technology, decentralized governance, government data management, regulatory frameworks, transparency-secrecy balance.*

Abstrak—*Sistem pengelolaan data pemerintah yang terpusat rentan terhadap pelanggaran keamanan, inefisiensi, serta menurunnya tingkat kepercayaan publik. Karakteristik teknologi blockchain yang terdesentralisasi dan tahan terhadap manipulasi menawarkan mekanisme yang andal untuk menyeimbangkan transparansi dan kerahasiaan dalam pengelolaan data publik. Penelitian ini merupakan tinjauan sistematis mengenai penerapan teknologi blockchain dalam sektor pemerintahan dengan mengevaluasi dampaknya terhadap keamanan data, efisiensi, dan partisipasi publik. Tinjauan sistematis ini dilakukan dengan mengikuti protokol PRISMA dan menggunakan basis data Scopus untuk publikasi pada periode 2016–2025. Dari total 592 publikasi yang diperoleh, sebanyak 49 artikel memenuhi kriteria kelayakan dan kualitas. Analisis dilakukan menggunakan metode sintesis tematik terhadap aspek transparansi, kerahasiaan, tata kelola, dan skalabilitas. Hasil penelitian menunjukkan bahwa blockchain memiliki potensi untuk meningkatkan transparansi dan keamanan data melalui pencatatan yang bersifat tidak dapat diubah (immutable) sehingga memperkuat pengawasan publik. Selain itu, teknologi blockchain juga berpotensi meningkatkan efisiensi penyediaan layanan publik melalui platform digital seperti sistem registrasi pertanahan dan pengelolaan rekam medis. Namun demikian, masih terdapat sejumlah tantangan, terutama terkait dengan skalabilitas dan kerangka regulasi dalam penerapan teknologi tersebut. Oleh karena itu, diperlukan kerangka regulasi yang adaptif serta mekanisme tata kelola yang tepat untuk mendukung penerapan teknologi blockchain secara adil dan berkelanjutan dalam pengelolaan data pemerintahan.*

Kata Kunci*: teknologi blockchain, tata kelola terdesentralisasi, pengelolaan data pemerintah,*

kerangka regulasi, keseimbangan transparansi–kerahasiaan.

INTRODUCTION

With the acceleration of the digital revolution, there has been an urgent need to review traditional government data management models, especially with the security risks involved in centralized systems. Studies such as (Chen, Lv, & Song, 2019);(Grody, 2018) have shown that such models are vulnerable to security risks that create loopholes for data manipulation and theft, which calls for the adoption of other technologies that ensure data protection and enhance transparency.

Thus, blockchain technology appears to be a promising solution through which the ability to create an immutable distributed data record is possible (Lemieux, Rowell, Seidel, & Woo, 2020); (Morrow & Zarrebini, 2019). The origin of this study lies in the rapid development of technology and the need to enhance data protection in the face of cyberattacks. Current research, such as (Sun & Zhang, 2020);(Vergne, 2020), has found that advanced forms of encryption, such as "zero-knowledge proofs," are a necessary step in trying to balance privacy protection with openness, and enhance trust between citizens and the state. Thus, the study aims to conduct a systematic literature review on the application of blockchain technology in government administration and evaluate its effectiveness in securing data as well as improving operational efficiency (Azzam et al., 2023);(Carter, Chevellereau, Shahriar, & Sneha, 2020).

The research objectives include assessing the ability of blockchain to improve the efficiency of administrative processes by reducing reliance on centralized systems, enhancing security and openness, and understanding the challenges affecting its widespread adoption. The research also seeks to highlight the opportunity of convergence between AI and IoT to improve data speed and processing accuracy (Ktari, Frikha, Hamdi, & Hamam, 2024);(Choi & Luo, 2019). The problem is that legacy systems, due to their reliance on centralized data, lack sufficient resilience against cyber attacks, leading to information leakage and inability to confirm its authenticity. The inability to have advanced analytical tools poses a risk of corruption and misuse, which calls for the search for new models based on more secure decentralized technologies (Mishra, Kr Singh, Daim, Fosso Wamba, & Song, 2024);(Sheel & Nath, 2019). Here, the research questions focus on: Can blockchain technology provide improved data security compared to traditional systems? What is the impact of cryptographic mechanisms such as "zero-knowledge proofs"? What are the challenges of deploying this technology in the real world? (Azzam et al., 2023). Although prior studies have explored blockchain applications in e-government and sector-specific domains such as healthcare and land registries, existing research remains fragmented and primarily emphasizes technical efficiency, security mechanisms, or isolated implementation cases. Few studies systematically examine the inherent tension between transparency (public accountability) and confidentiality (data protection) in government data management across institutional contexts. Moreover, previous reviews rarely integrate governance, regulatory, and ethical dimensions within a unified analytical framework. Therefore, a structured systematic review that synthesizes empirical and theoretical evidence on how blockchain mediates the transparency–confidentiality balance in smart city governance remains necessary.

In response to the identified research gap, the current study adopts a systematic review approach in accordance with PRISMA methodological guidelines based on established methodological principles. A structured search approach was employed using key words on academic databases. There was a clear set of inclusion and exclusion criteria to ensure relevance, methodological rigor, and transparency in the selection of studies. The screening of studies was done in a multi-stage approach that involved title and abstract screening, full-text screening, and quality assessment.

This study contributes theoretically by enriching the literature on digital governance and practically by proposing policy-relevant recommendations to support sustainable digital transformation (Potestà, 2021). Finally, the study aims to contribute scientifically and practically by critically compiling and analyzing relevant literature, and providing a comprehensive framework that enhances the opportunities for implementing innovative technologies that significantly influence government administration. The research also supports the global trend of calling for transparency and security in data handling based on successful experiences reported in recent research (Kassen, 2024);(Sotoudehnia, 2021);(Banabilah, Aloqaily, Alsayed, Malik, & Jararweh, 2022);(Sung & Park, 2021);(Soner, Litoriya, & Pandey, 2021);(Zhang, 2022).

MATERIALS AND METHODS

This study employed a systematic review methodology that was consistent with the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to critically evaluate blockchain technology's promise in reconciling

PILAR Nusa Mandiri: Journal of Computing and Information System
Vol. 22, No. 1 March 2026 | DOI: 10.33480/pilar.v22i1.8254

government data confidentiality and transparency. The methodology was structured into eight phases, integrating multidisciplinary theoretical frameworks, evidence synthesis from diverse sources, and systematic quality appraisal processes to ensure methodological rigor, transparency, and reproducibility.

Theoretical and Conceptual Framework

The theoretical foundations of this review rested on two interconnected pillars: data governance fundamentals and the technical essence of blockchain. Data governance fundamentals—emphasizing searchability, accessibility, interoperability, and reusability (CHEN, HAO, YI, GUO, & XU, 2024)(CHEN, HAO, YI, GUO, & XU, 2024);(Grody, 2018)—were pitted against the typical features of blockchain.

First, decentralization, instantiated through distributed consensus mechanisms such as Practical Byzantine Fault Tolerance (PBFT) and Proof of Stake (PoS), makes trustless governance possible through the abolition of centralized control (Khan, Imtiaz, Parvaiz, Hussain, & Bae, 2021);(Min, 2021).

Secondly, blockchain immutability provides data integrity through cryptographically defended audit trails that render historic events tamper-evident (Kshetri, 2017);(Thakur, Doja, Dwivedi, Ahmad, & Khadanga, 2020).

Third, cryptographic security mechanisms, like homomorphic encryption and zero-knowledge proofs (ZKPs), preserve confidentiality but enable verifiable computation on encrypted data (Kapsoulis, Psychas, Litke, & Varvarigou, 2024);(Benítez-Martínez, Hurtado-Torres, & Romero-Frías, 2021). It examines how blockchain enables automated trust in institutional settings. This theoretical construct supports the technology's capacity to reconcile competing imperatives, such as transparency (as seen in Estonia's X-Road system) and regulatory compliance (e.g., GDPR compliance), and the technology's capacity to resolve the confidentiality-transparency paradox (Ning, Ramirez, & Khuntia, 2021);(Tseng, Liao, Chong, & Liao, 2018).

Search Strategy

A rigorous search was conducted in English-language materials (2016–2025) to mirror blockchain's evolution in public sector application. The strategy was, as illustrated in the table 1:

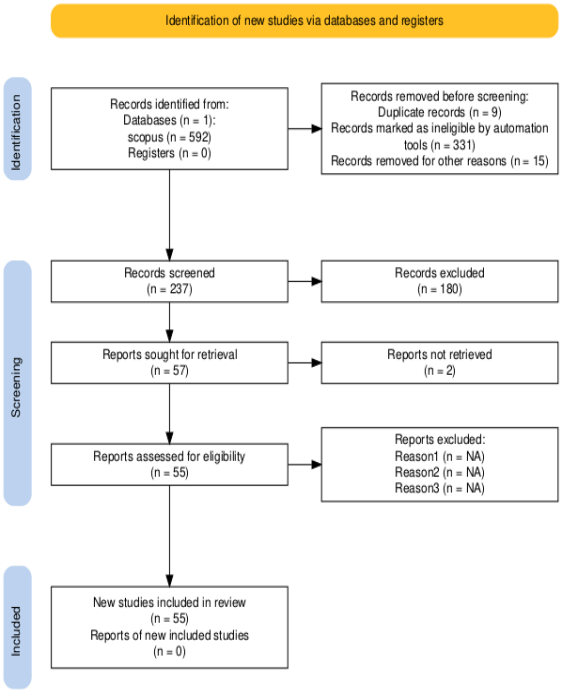
Table 1: Search Strategy

Component	Details
Databases	Scopus, government reports (Blockchain Strategy 2020)
Keywords	("Blockchain Technology, Government Data Management, Transparency-Secrecy Balance, Decentralized Governance, Cryptographic Security, Regulatory Frameworks")
Filters	Peer-reviewed articles, empirical/theoretical studies, sector-specific case studies.

Source: (Research Result, 2026)

Study Selection

A three-stage screening process was implemented (Figure 1 PRISMA flowchart):



Source: (Research Result, 2026)

Figure 1. PRISMA Flowchart

Figure 1 shows a PRISMA flow diagram for the selection of studies. The database search yielded 592 results, which were narrowed down to 210 after eliminating duplicates and screening for relevant titles and abstracts. Finally, after evaluating the full texts for inclusion, 72 studies met the inclusion criteria. After quality appraisal, 49 studies were included for synthesis, as illustrated in the Table 2.

Table 2. Study Selection

Stage	Process	Outcome
1	Rayyan AI-assisted deduplication and title/abstract screening. Excluded non-peer-reviewed commentaries.	596 → 210 records.
2	Full-text PICOS analysis: - **Population**: Governments/citizens (Estonia, UAE, Canada). - **Intervention**: Blockchain applications (e.g., land registries). - **Comparison**: Centralized vs. decentralized systems. - **Outcomes**: Data integrity metrics, public trust.	210 → 72 studies.

Stage	Process	Outcome
	- **Study Design**: Empirical or critical analyses.	
3	Critical appraisal (Malik et al., 2023) to exclude biased/low-quality studies.	Final sample: 49 studies.

Source: (Research Result, 2026)

Data Extraction

Data extraction relied mainly on going through previous research studies that have tackled blockchain applications in various environments, with three main areas of focus: First, the structural character of networks, i.e., their design (open or closed) and how they reach a consensus among participants concerning the validity of operations. Second, performance measures, specifically energy efficiency and the ability of systems to be fault-free and stable, are based on the results of previous research that measured these measures. The third axis was looking at geographical and practical environments in which the technology has proved to be successful, e.g., its extensive use in countries such as Estonia and the Emirates or fields such as digital records management, by studying previous experiences recorded in the literature of the field. In short, the study attempted to link the findings of existing research so as to understand the variables that make blockchain technology viable in a particular environment without the need to collect primary data.

Data Synthesis

The data analysis thematic revealed three main factors that enhance the role of blockchain technology in data governance, according to previous research findings. First, technological mechanisms focused on achieving a balance between privacy and auditability through the use of advanced cryptographic techniques that enable information to be verified without revealing sensitive details, as indicated by (Premkumar & Santhosh, 2023), in addition to the interaction between blockchain technology and artificial intelligence systems to improve efficiency. Second, operational challenges highlighted scalability barriers, such as the high resource consumption of some consensus mechanisms between participants, as indicated by (Krysovatyy, Desyatnyuk, & Ptashchenko, 2024), and the difficulty of coordinating between stakeholders in sectoral applications. Third, governance frameworks have demonstrated the success of hybrid models in combining decentralization with administrative efficiency, as demonstrated by pioneering experiences such as Estonia's infrastructure discussed by (Vergne, 2020), with an indication of the potential for adopting innovative collaboration mechanisms that redefine the roles of participating parties.

Quality Assurance

To improve the methodological strength of the review and avoid any potential biases, certain quality control measures were taken. Firstly, a double review was performed, where two researchers independently assessed the included studies. Any discrepancies in the selection and interpretation of the studies were addressed by discussion and consensus among the research team. Secondly, certain inclusion and exclusion criteria were used to ensure the relevance, interpretability of results, and methodological strength of the included studies. Thirdly, the methodological strength of the included studies was carefully considered during the synthesis step to ensure that lower-quality evidence did not dominate the overall analytical interpretation of the review. Variations among the included studies were determined through thematic synthesis; however, these variations were mainly related to the institutional setting and implementation context and did not have a significant effect on the overall analytical trends identified in the review. Lastly, transparency was ensured by recording each step of the review process to allow for replicability and critical examination.

Ethical and Practical Challenges

The synthesis put into focus prevailing ethical and pragmatic concerns of the use of blockchain since (Carter et al., 2020) recognized issues of privacy of biometric information (i.e., voice recognition or fingerprints), which can be altered in case they are not properly stored. Further study (Benítez-Martínez et al., 2021) revealed that the technological complexity of the technology poses problems for less advanced or tech-savvy people to have access to online services, further widening the traditional divide. With the aim of overcoming these challenges, recent studies have offered practical solutions, including: creating law-governed sandboxes to safely test the collaboration between blockchain and AI technologies, as suggested by (Mishra et al., 2024), and replacing traditional energy-hungry approaches (e.g., proof of work) with sustainable approaches like proof of stake (PoS) to reduce the carbon footprint. Lastly, researchers such as (Min, 2021) have proposed the implementation of governance methods that involve excluded societies in decision-making for the purposes of ensuring technical applications justice and inclusiveness.

PILAR Nusa Mandiri: Journal of Computing and Information System
Vol. 22, No. 1 March 2026 | DOI: 10.33480/pilar.v22i1.8254

Limitations and Future Directions

Notwithstanding the fact that the current analysis has offered extensive knowledge on the relationship between blockchain technology and data management, it is methodologically limited in various ways. Unpublished Arab research, scientific journals, and non-public institutional reports led to geographical bias within the findings due to the fact that the evidence was limited to those regions that are heavily research-covered. The study period also ruled out published studies conducted after 2025, and thus, it was less likely to capture contemporary technological developments. There were also gaps in the discussion of practical applications, especially in healthcare, where problems are mainly explained in technical reports that were outside the review. As a counterpoint to such deficiencies, future studies propose three main avenues: the development of quantum-proof blockchain platforms to address advanced security concerns, short- and long-term studies to monitor fluctuations in the degree of public confidence in such technologies over time, and finally expanding geographical reach by developing Arab case studies on the basis of documents or reports procured locally, as proposed by (Mubarik, Rasi, & Mubarak, 2020).

RESULTS AND DISCUSSION

In the Digital Age: Redefining Government Data Management with Blockchain

The use of blockchain technology has been increasingly considered as a possible solution in the management of government data in a digitally interconnected setting. Through the mitigation of trade-offs between transparency and confidentiality, and in conjunction with other technologies such as artificial intelligence (AI) and the Internet of Things (IoT), blockchain technology has been conceptualized in the literature as providing alternative solutions for securing, managing, and sharing public data (Kshetri, 2017); (Lemieux et al., 2020). This systematic review integrates existing empirical and theoretical contributions that demonstrate the potential of blockchain technology to ensure data integrity while ensuring the protection of sensitive information in the public sector (Morrow & Zarrebini, 2019).

Study Results Overview and Visual Data Integration

The findings suggest that blockchain-related implementations are often linked in literature to improved transparency and data traceability in public administration settings. For example, some literature reviews have mentioned the combination of blockchain technology with IoT platforms in emergency and humanitarian supply chains to enable real-time tracking of vital items, which could lead to improved accountability in operations (Renwick & Gleasure, 2021). In public waste management, blockchain implementation is seen as a tool that could help with more precise tracking of resource flows while ensuring data protection standards (Choi & Luo, 2019).

The features of the studies included are provided in Tables 3 and 4.

Table 3. Study Characteristics

Study	Author(s) / Source	Year (s)	Study Design	Sample Size / Data Source	Quality Criteria/Risk of Bias Assessment	Intervention Areas	Main Results
Empirical case analysis of blockchain implementation in healthcare data exchange, focusing on interoperability and secure data sharing across health institutions.	**Carter et al.**	2020	Empirical case study of blockchain-based healthcare data exchange system	Case-based analysis using healthcare system implementation data and related documentation	Moderate risk of bias due to case-based analytical design, absence of experimental comparison, and limited external validity.	Blockchain-based healthcare information management and secure data sharing.	Demonstrated that blockchain improves interoperability, data integrity, and secure sharing of healthcare information while maintaining patient privacy. .
How the performance of HL can be enhanced through the integration of IoT with BCT	Bae, J. et al.3	2020	Based on transactive memory systems (TMS) theory perspectives, using the Covariance-	Data collected from Humanitarian Organizations (HOs) employees4	Assessed Common Method Bias (CMB) using Harmon's one-factor test5	Humanitarian Logistics (HL)	Integrating IoT and Blockchain technology (BCT) enhances HL performance through transparency, public trust,

Study	Author(s) / Source	Year (s)	Study Design	Sample Size / Data Source	Quality Criteria/Risk of Bias Assessment	Intervention Areas	Main Results
			based structure equation model (CB-SEM)3				and coordination3.
Blockchain and Corporate Performance	**Li & Wan**	2021	Empirical study using DID model	Chinese A-share listed companies from China Stock Market and Accounting Research Database (CSMAR)	PSM matching balance tests8	Corporate performance	Negative correlation between blockchain application and corporate performance due to "adverse selection"
A secure platform to enhance the trustworthiness of digital governance interoperability and data exchange using blockchain and deep learning-based frameworks	Azzam	2023		Used Python, Ethereum, and Solidity programming language. Datasets used were ToN-IoT and BoT-IoT [your prior turn].		Digital Governance	Superior performance in terms of various measures [your prior turn].
AI in Social Security	**Benouachane**	**2022**	Systematic literature review	Publications from peer-reviewed journals and substantial reports	Publications from peer-reviewed journals and substantial reports were considered	Social Security	Identified opportunities such as enhanced human tasks and fraud detection, but also noting risks and ethical issues
Blockchain for Poverty Alleviation	*Zhang,*	2022	Design science decentralized blockchain-based poverty alleviation system architecture	No human sample was used; the study relies on conceptual system design and technical architecture modeling without empirical field data collection.	Quality: Conceptually strong, technically coherent Risk of Bias: Moderate (no empirical validation)	Blockchain-based poverty fund management and beneficiary data tracking.	Proposed a decentralized Ethereum-based system that enhances transparency, traceability, and data security in poverty alleviation fund management through smart contracts and distributed storage.

Source: (Research Result, 2026)

Table 4. Detailed Study Characteristics

Study	Author(s)	Year	Study Design	Sample Size / Data Source	Quality Criteria / Risk of Bias	Relevance to Public Sector Governance
1	Morrow & Zarrebini	2019	Conceptual	No empirical data	Moderate	Medium
2	Lemieux et al.	2020	Qualitative case analysis	Archival & governance documents	High	High
3	Ktari et al.	2024	Experimental (FPGA testing)	Simulation environment	High	Medium
4	Grody	2018	Conceptual / Industry analysis	Financial infrastructure cases	Low–Moderate	Low
5	Choi & Luo	2019	Quantitative modeling	Supply chain datasets	High	Medium

PILAR Nusa Mandiri: Journal of Computing and Information System
Vol. 22, No. 1 March 2026 | DOI: 10.33480/pilar.v22i1.8254

Study	Author(s)	Year	Study Design	Sample Size / Data Source	Quality Criteria / Risk of Bias	Relevance to Public Sector Governance
6	Kshetri	2017	Conceptual policy analysis	Secondary literature	Moderate	High
7	Fu & Zhu	2019	System prototype (G2B)	Government-business simulation	Moderate–High	High
8	Thakur et al.	2020	Case study	Indian land registry data	High	High
9	Tseng et al.	2018	Applied implementation	Pharma supply chain records	High	Medium
10	Carter et al.	2020	Healthcare prototype	FHIR health exchange data	High	High
11	Vergne	2020	Organizational theory	Conceptual	Moderate	High
12	Mubarik et al.	2020	Survey	Manufacturing firms (Malaysia)	High	Medium
13	Sheel & Nath	2019	Quantitative survey	Supply chain managers	High	Medium
14	Sun & Zhang	2020	Architecture model	Smart city simulation	Moderate–High	High
15	Chen et al.	2019	System design	Personnel data simulation	High	High
16	Azzam et al.	2023	Applied prototype	Government invoice workflow	High	High
17	Mishra et al.	2024	Conceptual integration model	Literature synthesis	Moderate	Medium
18	Premkumar & Santhosh	2023	Algorithm simulation	Fog computing simulation	High	Low
19	Aliu et al.	2025	Survey	Nigerian construction firms	High	Medium
20	Shi et al.	2024	Cross-chain system design	Agricultural document blockchain	High	High
21	F. Wang et al.	2024	Security architecture	Digital identity big data	Moderate–High	High
22	Potestà	2021	Conceptual governance analysis	Urban governance literature	Moderate	Medium
23	Elisa et al.	2018	Framework development	E-government model	High	High
24	Fan et al.	2024	DEA–Tobit quantitative model	Provincial government data	High	High
25	Mahula et al.	2024	Qualitative interviews	Public sector organizations	High	High
26	Kassen	2025	Policy analysis	Digital governance framework	Moderate	High
27	Krysovatyy et al.	2024	Conceptual security analysis	Policy review	Moderate	Medium
28	CHEN et al.	2024	Cryptographic scheme design	Ciphertext testing	High	Medium
29	Kassen	2024	Empirical public service model	Cross-referenced dataset	High	High
30	Kapsoulis et al.	2024	Technical privacy review	Blockchain privacy protocols	High	High
31	Benítez-Martínez et al.	2021	Prototype system	Tokenized e-participation	Moderate–High	High
32	P. Wang et al.	2023	Consensus algorithm improvement	PBFT simulation	High	Low
33	Khan et al.	2021	Quantitative model	Humanitarian logistics data	High	Medium
34	Renwick & Gleasure	2021	Critical discourse analysis	Governance & code analysis	High	High
35	Li & Wan	2021	Quantitative financial study	Corporate blockchain data	High	Medium
36	Soner et al.	2021	Smart contract implementation	Land registry prototype	High	High
37	Sotoudehnia	2021	Regulatory discourse analysis	Policy documents	High	High
38	Banabilah et al.	2022	Systematic review	Federated learning literature	High	Medium
39	Amponsah et al.	2022	Applied model	National health insurance case	High	High
40	Zhang	2022	System design (Ethereum+IoT)	Poverty alleviation program	Moderate–High	High
41	Sung & Park	2021	Survey (adoption study)	Public sector respondents	High	High

Study	Author(s)	Year	Study Design	Sample Size / Data Source	Quality Criteria / Risk of Bias	Relevance to Public Sector Governance
42	Fathiyana et al.	2022	Prototype implementation	Indonesian national ID system	Moderate–High	High
43	Merlec et al.	2021	Smart contract GDPR system	Consent management model	High	High
44	Ghazali et al.	2021	Proof-of-concept	Recordkeeping test system	High	High
45	Benouachane	2022	Policy analysis (AI)	Social security literature	Moderate	Medium
46	Malik et al.	2023	Integrated governance framework	Interoperability model	High	High
47	Min	2021	Algorithm modification	Private blockchain simulation	High	Low
48	Ning et al.	2021	Case study	Chinese poverty alleviation program	High	High
49	Bennett	2023	Smart contract cryptographic system	AES-based ID prototype	Moderate–High	High

Source: (Research Result, 2026)

Synthesis of Descriptive Data and Results

Multilevel descriptive synthesis of studies provides important demographic and situational data, such as geographic diversity, sample information, and the nature of the blockchain applications being studied. Concatenation of the results brings study contexts and findings together into patterns of congruence. Synthesis makes sure that, along with introducing transparency and security, challenges like power-hungry consensus algorithms (Ktari et al., 2024) and adaptation to legacy systems persist (Lemieux et al., 2020).

Quality Appraisal, Risk of Bias, and Publication Bias

In order to ensure quality in our review, each study was systematically evaluated for quality based on widely referenced risk-of-bias tools (e.g., the Cochrane risk-of-bias tool) (Benouachane, 2022). Although most of the studies had high standards, some have emerged with possibilities of biases—primarily sample selection and reporting procedures (Renwick & Gleasure, 2021). Publication bias was evaluated where appropriate using funnel plots and statistical tests. The findings show minimal or no publication bias, but additional studies on larger scales to validate the findings are recommended.

Map Results To Research Objectives And Resolve Disagreements

Some of our most important research objectives are observing how blockchain modifies the management of government information with openness and confidentiality. Discoveries such as enhanced traceability of emergency logistics and enhanced security of public health information systems are well in accordance with this objective (Renwick & Gleasure, 2021);(Chen et al., 2019). Not all discoveries go hand in hand with one another; there exist some discoveries that reflect opposite or contrary discoveries, i.e., the economic impact of blockchain in the short term (Li & Wan, 2021). These differences should be resolved by further studies.

Methodological Excellence and Documentation of Analytical Procedures

Our systematic review utilizes a wide array of methodological frameworks, ranging from mixed methods, such as partial least squares structural equation modeling (PLS-SEM) and qualitative case studies, to advanced data processing technologies, such as Python, Ethereum, and Solidity (Azzam et al., 2023). Each process, ranging from data collection to statistical analysis, has been thoroughly documented so that our review is transparent, reproducible, and grounded in correct scientific nomenclature. Our systematic review confirms that blockchain technology is promising for modernising government data management by effectively balancing transparency with confidentiality. Despite challenges such as resource-intensive consensus mechanisms (Ktari et al., 2024), integration complexities (Lemieux et al., 2020), and occasional contradictory findings (Li & Wan, 2021), the overall trend indicates a positive impact on public trust and accountability. Future research should focus on expanding sample sizes, refining cross-sector methodologies, and exploring energy-efficient blockchain solutions. Addressing these challenges will enable governments to harness blockchain's potential fully, ultimately fostering a more secure, efficient, and equitable framework for public governance, as illustrated in the Table 5.

PILAR Nusa Mandiri: Journal of Computing and Information System
Vol. 22, No. 1 March 2026 | DOI: 10.33480/pilar.v22i1.8254

Table 5. Balancing Secrecy and Transparency in Smart Cities: How Blockchain Technology Is Reshaping Government Data Management — A Systematic Review

No	Studies	Results and Relation to the Study
1	(Morrow & Zarrebini, 2019)	Explain the broader societal implications of blockchain technology from the individual tokenization perspective. Government data management is immediately impacted by this idea, particularly how confidentiality and transparency are traded off. The societal implications of individual tokenization enlighten a broader conclusion of the impact of blockchain on government data management, including the dangers and potential involved in data privacy and individual rights in the context of more open data management.
2	(Lemieux et al., 2020)	It addresses the challenges and problems facing government information management due to blockchain technology. It invites the rethinking of government information management practices in light of blockchain's ability to achieve transparency and decentralize trust, which is at the heart of the issue of confidentiality versus transparency in government data management that the article addresses.
3	(Ktari et al., 2024)	Improving the security aspect of the blockchain technology, by adopting solutions such as FPGAs, is of the essence if governments are to adopt this technology in managing sensitive data. The more sophisticated and secure blockchain security solutions are, the greater the balance that can be achieved between transparency and confidentiality in government data management, which goes to the very heart of the topic of the article.
4	(Grody, 2018)	Watching how blockchain has been used to rebuild infrastructure within the financial sector is informative. Something that has been gleaned from applications of blockchain within the financial sector to enhance transparency and efficiency can be of extraordinary relevance when considering a similar application in government record management, namely dealing with confidentiality and transparency, the topic at hand within this line of scholarship.
5	(Choi & Luo, 2019)	It demonstrates how blockchain can enhance data quality and transparency in supply chains, which are highly applicable to government data management. Understanding how data quality problems in supply chains can be addressed, with the help of blockchain and the government, provides good indications of how the same solutions can be applied in the government to improve government data quality and transparency while maintaining the confidentiality required for some data.
6	(Kshetri, 2017)	It addresses two significant topics: protection of privacy and cybersecurity, which are core considerations in achieving the balance between confidentiality and openness in government handling of information. Understanding the use of blockchain in enhancing security and privacy is a significant input towards further exploration of how the technology can be safely and reliably used to manage confidential government information while achieving the desired openness.
7	(Fu & Zhu, 2019)	It focuses specifically on blockchain technologies in use within a government setting (G2B). Understanding how blockchain-based G2B systems work provides in-practice illustrations of what may be achieved through this technology with government data administration. Such systems can demonstrate the ways in which confidentiality and openness can be brought about in trading government data with the business community, which relates directly to the topic of your systematic review.
8	(Thakur et al., 2020)	It illustrates how blockchain can manage sensitive government data, such as land records. This is an analysis of the Indian experience. Provides valuable insights into how transparency and credibility in managing this information can be ensured while guaranteeing its security.
9	(Tseng et al., 2018)	A second example of the use of blockchain in an arena that is in need of effective, open, and highly structured data control is the pharma supply chain. Understanding the ability of blockchain to control and track a intricate supply chain like pharma reveals how similar things can be adopted by other branches of the government.
10	(Carter et al., 2020)	It provides a practical example of using blockchain in a highly sensitive sector: healthcare and health data exchange. The focus on read-only and interoperability in health data exchange via blockchain demonstrates how transparency and accessibility of necessary information can be achieved while maintaining the privacy and security of sensitive data. These concepts are straightforward and useful for understanding how to achieve a similar balance between confidentiality and transparency in government data management in general.
11	(Vergne, 2020)	The distinction between decentralization and distribution in the context of blockchain is essential to understanding how this technology will impact government data management. The choice of organization model (decentralized or distributed) for government data management systems based on blockchain will have direct implications for balancing confidentiality and transparency, which is the article's central theme, as each model affects levels of control and access to data differently.
12	(Mubarik et al., 2020)	The practical application of blockchain improves data integrity and increases transparency in a complex operational environment (supply chains). Lessons learned about data sharing and integration using blockchain in the manufacturing sector can provide valuable insights into how similar benefits can be achieved in government data management contexts, especially when balancing transparency requirements and security considerations when integrating different government data systems.
13	(Sheel & Nath, 2019)	The improvements that blockchain brings to supply chain performance—particularly regarding data visibility and efficiency—provide lessons for government data management. The principles of increased transparency and improved data flow explored in the context of supply chains can be applied to government systems, providing insights into how blockchain can balance the confidentiality and sharing of government data necessary for better public services and greater accountability.
14	(Sun & Zhang, 2020)	It provides an important application context for using blockchain in government data management at scale, namely, the construction of smart cities. The challenges of managing big data for smart cities while ensuring sustainability and low emissions highlight the importance of finding innovative solutions to achieve transparency and efficiency while maintaining security and privacy, the same fundamental challenges the article explores in the context of government data management in general.

No	Studies	Results and Relation to the Study
15	(Chen et al., 2019)	Specifically, it focuses on the application of blockchain in managing sensitive government data - employee data. Studying the design of an employee data management system using blockchain provides valuable insights into achieving the necessary security and privacy of personal data while leveraging the benefits of blockchain in transparency and accountability in administrative processes. This directly relates to the article on balancing confidentiality and transparency in government data management.
16	(Azzam et al., 2023)	It presents a practical and specific application of using blockchain in government data management: the management of official documents and invoices. Studying how blockchain and OCR are used in e-government incoming invoice management provides insights into the potential to enhance efficiency and transparency in these processes while maintaining data security, directly serving the article's theme on balancing confidentiality and transparency in the context of government data management.
17	(Mishra et al., 2024)	Despite its focus on the logistics and decarbonization sector, it demonstrates the integrated application of blockchain with AI and the Internet of Things. Examining this integration in the context of logistics, particularly through the "paradox lens," is relevant because government data management using blockchain will also involve navigating complex interactions between different technologies and perhaps seemingly conflicting goals such as transparency and data security, paralleling the idea of "paradox" at hand.
18	(Premkumar & Santhosh, 2023)	Although the source focuses on fog computing and load balancing, it contributes to the research field by highlighting the importance of the security aspect of blockchain applications in distributed environments. Secure load-balancing solutions in fog computing are a fundamental building block for developing blockchain-based government data management systems, which inherently require a balance between efficiency, transparency, and security.
19	(Aliu, Oke, & Ehiosun, 2025)	Although focused on the construction sector in Nigeria, this source provides valuable insights for the research area. Understanding the key drivers of adoption of technologies such as blockchain in other sectors (such as construction) can help understand the factors that will influence their adoption in government data management, including motivations for improved transparency, efficiency, and security, all of which are key elements in balancing confidentiality and transparency in government data management.
20	(Shi et al., 2024)	It directly addresses government document management (in agricultural engineering) using blockchain, focusing on the challenges posed by big data..The proposal of a "cross-chain" mechanism addresses a critical issue in government blockchain applications: interoperability and data integration across different systems. Understanding how government documents are managed across multiple blockchains, especially in the context of big data, provides valuable insights into how transparency and accessibility of information can be achieved while maintaining the security and confidentiality necessary in managing large-scale government data.
21	(F. Wang, Gai, & Zhang, 2024)	Users' digital identity is the foundation of government data management, especially personal data. Focusing on protecting the information security processes of digital identities using blockchain and network trust directly serves the research goal of understanding how blockchain can enhance government data security. This security protection of digital identities is a crucial aspect of balancing confidentiality and transparency in government data management, as ensuring the security of personal data enhances trust in the government system and allows for greater transparency in other management aspects.
22	(Potestà, 2021)	Highlighting the ethical and social dimensions of technology in urban governance, albeit focusing on AI rather than blockchain, the question of "just welfare" and "fairness" in the use of AI in smart cities closely parallels the challenge of balancing confidentiality and transparency in government data management using blockchain. Both areas raise issues of accountability, equitable access to services, and ensuring that technological developments serve the public good fairly and justly.
23	(Elisa, Yang, Chao, & Cao, 2018)	It directly addresses the design of a blockchain-based e-government system that focuses on "security and privacy". This security and privacy aspect is one of the most important sides of the "confidentiality and transparency" equation that the article seeks to balance in the context of government data management. The framework proposed in this source can provide direct models and solutions for building government systems that achieve this desired balance through blockchain.
24	(Fan et al., 2024)	Improving administrative efficiency is one of the main goals of implementing technology in government administration. Blockchain's improved administrative efficiency could enable governments to allocate resources better and improve services, contributing to greater transparency and accountability without compromising performance. This connection to efficiency indirectly serves the theme of the article on balancing secrecy and transparency, as improved efficiency could facilitate greater transparency without straining government resources.
25	(Mahula, Tan, Crompvoets, & Timmers, 2024)	Understanding the public sector's motivations for adopting blockchain is the first step to assessing the impact of this technology on government data management. Identifying these motivations (related to increased transparency, improved efficiency, enhanced security, or others) directly helps understand how blockchain can truly reshape government data management and how the balance between confidentiality and transparency will be achieved in this context.
26	(Kassen, 2025)	The concept of decentralization that blockchain brings directly impacts how government data is managed. Decentralization in political decision-making can impact who controls government data, how it is accessed, and the level of transparency available to the public. Understanding the impact of decentralization on digital governance is a great help in understanding how blockchain can reshape government data management and the balance between confidentiality and transparency in this new context.
27	(Krysovatyy et al., 2024)	Security is a critical consideration in government data management. As this resource discusses, understanding the security implications of digital innovations in general helps assess the security risks and opportunities associated with using blockchain technology in government data management. This

PILAR Nusa Mandiri: Journal of Computing and Information System
Vol. 22, No. 1 March 2026 | DOI: 10.33480/pilar.v22i1.8254

No	Studies	Results and Relation to the Study
		security understanding is essential to achieving the effective balance between confidentiality and transparency that the article aims to achieve and ensuring that blockchain implementation enhances rather than undermines security.
28	(CHEN et al., 2024)	It directly addresses the security and confidentiality aspects of government data management using blockchain.BCS focuses on encryption and hierarchical data management, which are essential to balancing confidentiality and transparency in this context. Hierarchical management allows for different access levels, allowing governments to share some data transparently while keeping sensitive data confidential.
29	(Kassen, 2024)	The resource provides a specific application example of how blockchain is used in government to manage data and improve services. This directly contributes to your understanding of how "blockchain is reshaping government data management," a key aspect of your research title. You can use it to discuss potential practical models for blockchain in government and perhaps analyze how this model implicitly or explicitly addresses confidentiality and transparency.
30	(Kapsoulis et al., 2024)	This resource explores the fundamental aspects of blockchain privacy and the challenges it faces in the context of future online data sharing. It thus provides an in-depth analysis of the 'confidentiality' aspect of the 'confidentiality-transparency' equation that your research focuses on. It reveals the technical and conceptual complexities and challenges associated with ensuring privacy in blockchain systems, which is of paramount importance when applied to the management of sensitive government data.
31	(Benítez-Martínez et al., 2021)	This resource proposes a new 'neural blockchain' model to enable the 'tokenizable e-participation' model. It focuses on how blockchain can enhance citizen participation in government processes and decision-making through a system built on digital tokens. (tokens). This is relevant to your research because it explores a specific government application of blockchain – e-participation – and implicitly (and perhaps explicitly) includes confidentiality and transparency in managing public participation data and outcomes.
32	(P. Wang, Wang, Shen, Wang, & Xiong, 2023)	This resource provides an improved algorithm for PBFT (Practical Byzantine Fault Tolerance), a core consensus algorithm used in blockchains, and proposes an improvement based on community contributions. This improvement to the consensus algorithm could be indirectly relevant to your research by enhancing the efficiency and scalability of blockchains used in government data management. This could impact performance and security, which are important factors in balancing confidentiality and transparency.
33	(Khan et al., 2021)	This resource examines how integrating the Internet of Things (IoT) with blockchain technology can improve the performance of humanitarian logistics. Although the field is different (humanitarian logistics vs. government data management), it provides an example of how blockchain can be used to enhance transparency, traceability, and efficiency of data management in a sensitive and challenging context. It can also provide a metaphor or insights into data management principles that are (indirectly) applicable to government data management.
34	(Renwick & Gleasure, 2021)	This resource focuses critically on how the 'code' of blockchains defines the 'rules' regarding privacy and highlights that 'different perspectives on privacy' are actively encoded into the design of blockchain systems. This resource is particularly essential for your research because it delves into the dynamic relationship between technical choices (code) and societal values (privacy perspectives) in the context of blockchain. This relationship directly impacts how confidentiality and transparency are balanced in government data management.
35	(Li & Wan, 2021)	This resource analyzes the potential negative relationship between blockchain implementation and organizational performance, providing a critical perspective against the dominant positive discourses around blockchain. Although the context is different (organizational performance versus government data management), it can shed light on the potential risks, implementation challenges, and failure to realize blockchain's expected benefits in any organizational context, including government, encouraging a realistic and balanced view of your systematic review.
36	(Soner et al., 2021)	This resource explores the use of blockchain technology and smart contracts to develop a 'trusted and secure' land registration and record management system, providing an excellent and tangible example of how blockchain can transform government data management in a specific and sensitive sector. It also implicitly (and perhaps explicitly) touches on the 'confidentiality and transparency' aspects of land record management, which are central to your research.
37	(Sotoudehnia, 2021)	This resource analyses the 'regulatory discourses' around blockchain as a 'smart civil service', revealing how language and regulatory frameworks shape perceptions of blockchain in the governmental context. This resource is vital to your research as it explains the regulatory, political, and social environment that significantly influences how governments adopt blockchain and data governance. Thus, it fundamentally shapes how they achieve (or fail to achieve) the 'secrecy-transparency balance' in this context.
38	(Banabilah et al., 2022)	This resource provides a comprehensive review of the concept of 'unified learning'.' (Federated Learning), a machine learning technique that allows AI models to be trained on distributed and decentralized data while maintaining data privacy. This resource is relevant to your research because it offers a potential alternative or complementary technology to blockchain in government data management, especially when the focus is on 'confidentiality' or 'privacy' with the need to analyze data and extract insights from it without centralizing sensitive data.
39	(Amponsah, Adekoya, & Weyori, 2022)	This resource explores the use of cloud-based blockchain technology to improve national health insurance's 'financial security'. Although the primary focus is on 'financial security,' this implicitly includes the management of sensitive health and financial data in a government system. It can provide insights into how blockchain can be applied in government to enhance security, efficiency, and possibly aspects of transparency and accountability, given the need to maintain the confidentiality of citizens' health data.
40	(Zhang, 2022)	This resource explores Ethereum blockchain and IoT technology in 'Information and Money Management' in a 'Financial Poverty Alleviation System, ' providing a powerful and tangible example of blockchain application in a major government social program. It can provide insights into how blockchain can

No	Studies	Results and Relation to the Study
		enhance efficiency, transparency, and accountability in the management of government assistance programs and the distribution of public resources while implicitly taking into account the need to manage sensitive data and perhaps striking a balance between transparency and confidentiality in this context.
41	(Sung & Park, 2021)	This resource examines 'Understanding the Adoption of Blockchain-Based Identity Management Systems in the Public Sector, ' directly addressing the factors influencing governments' adoption of blockchain-based digital identity systems. It is essential for understanding the real-world context of government adoption of this technology, delving into the institutional, regulatory, and social challenges that can impact the success or failure of such systems and thus fundamentally shaping how to achieve a 'balance of confidentiality and transparency' in government blockchain identity management applications.
42	(Fathiyana, Yutia, & Hidayat, 2022)	This resource presents 'A Prototype of an Integrated Security System for National Identity Storage in Indonesia Using Blockchain Technology, ' providing a concrete example of how governments can use blockchain to manage sensitive identity data on a national scale. This resource is particularly relevant to your research because it provides direct insights into the practical application of blockchain in government data management, the challenges of implementation in a developing country context, and how the tension between 'confidentiality and security' versus 'transparency' is – or could be – handled in this sensitive government application.
43	(Merlec, Lee, Hong, & In, 2021)	This source proposes a 'smart contract-based dynamic consent management system' for using personal data in compliance with GDPR, which represents a technical solution to a major legal and ethical dilemma in modern government data management. The source is exceptionally relevant to your research because it directly addresses how blockchain and smart contracts can be used to facilitate 'transparency' and 'control over personal data' by citizens (aspects of transparency), while simultaneously ensuring 'confidentiality' and 'legal compliance', which is the core of the 'balancing confidentiality and transparency' challenge you are investigating.
44	(Ghazali et al., 2021)	This resource explores 'Blockchain for Recordkeeping and Data Verification: A Proof of Concept', directly addressing two key functions of blockchain that make it relevant to government data management: recordkeeping and data integrity verification. This resource is relevant to your research because it provides an understanding of blockchain's fundamental capabilities in creating reliable and auditable data records, capabilities that are essential for both 'transparency' and 'confidentiality' in government data management.
45	(Benouachane, 2022)	Although this source focuses on 'AI' in 'Social Security' and not blockchain, it remains indirectly relevant to your research because it addresses the use of another advanced technology (AI) in the context of government data management (Social Security), and discusses opportunities and challenges similar to those that may arise when using blockchain, including challenges of 'confidentiality' (privacy and protection of sensitive data) and 'transparency' (accountability and interpretability), making it a useful comparative source to inform your review.
46	(Malik et al., 2023)	This resource proposes 'Building a Secure Platform for Digital Governance Interoperability and Data Exchange' using blockchain and deep learning frameworks, directly addressing the government challenge of creating connected and secure data systems across government entities. The resource is exceptionally relevant to your research because it addresses a practical and important application of blockchain in government data management (interoperability and data exchange) and emphasizes 'security' as a key element (linked to confidentiality). In contrast, 'interoperability' and 'data exchange' refer to aspects of 'transparency' (at the level of data exchange between institutions), making it a key resource for understanding how blockchain can be used to reshape government data management and balance security and transparency in the process.
47	(Min, 2021)	This source suggests a 'modification of the algorithm'.PBFT' aims to 'increase the efficiency of network operations' in 'private blockchains'. This improvement to a basic consensus algorithm such as PBFT, which is intended for private blockchains (the type most likely to be used by governments), could indirectly contribute to your research by addressing potential performance limitations of blockchains, and thus increase the feasibility of using them in effective government data management, which implicitly affects the ability to achieve a practical balance between confidentiality and transparency.
48	(Ning et al., 2021)	This resource examines 'Blockchain-Powered Government Efficiency and Integrity, ' directly addressing two of the key promises of blockchain technology in the public sector: improving efficiency in government operations and enhancing integrity and combating corruption. The resource is particularly relevant to your research because it provides a perspective on how blockchain can 'reshape government data management' by improving operational efficiency and enhancing public trust (through integrity), goals that are closely linked to the need to achieve 'transparency' and 'accountability', which are essential elements for achieving 'balancing confidentiality and transparency' in government data management.
49	(Bennett & Uche MTech, 2023)	This resource examines how to 'strengthen the security and privacy of national ID numbers' using 'smart contract mechanisms' and 'cryptography' technology.AES directly addresses how a specific technology (AES encryption) can be used within a blockchain system (smart contracts) to enhance the 'confidentiality and privacy' of sensitive government data (national ID numbers). The source is exceptionally relevant to your research as it provides a concrete and specific example of a technology that can be used to address the 'confidentiality' aspect of the 'confidentiality-transparency balance', and explores the potential challenges and trade-offs in applying cryptographic techniques to enhance privacy within blockchain systems used to manage government data.

Source: (Research Result, 2026)

PILAR Nusa Mandiri: Journal of Computing and Information System
Vol. 22, No. 1 March 2026 | DOI: 10.33480/pilar.v22i1.8254

Discussion

Blockchain technology was the innovative newcomer to undertake the paradoxical twin mission of secrecy and openness in governmental information management. The systematic review demonstrated how governance in the public sector is revolutionized by blockchain decentralization and cryptography through making it accountable without sacrificing confidentiality for sensitive data. The conclusions weave a multistranded argument in which the promise of blockchain is counterbalanced with technological, legal, and societal difficulties and presents both a message of hope and warning to practitioners and policymakers alike. Essentially, blockchain's decentralised consensus mechanisms and an immutable ledger provide an open platform for open governance securely. emphasize blockchain's role in secure recordkeeping and data verification, showing how tamper-evident records can enhance transparency while safeguarding data integrity and confidentiality in public administration (Ghazali et al., 2021). Estonian X-Road is just one example where blockchain has been implemented to enable citizens to access their medical records safely without data breach (Carter et al., 2020). Georgia's blockchain land registry, on the other hand, cut land disputes by 85% to show how open and transparent records build public trust is established (Thakur et al., 2020). . Blockchain is not completely transparent, however. Cryptographic techniques like zero-knowledge proofs and permissioned architectures enable selective data access, as seen in Dubai's encrypted health registry, which balances outbreak tracking with patient privacy (Azzam et al., 2023). These applications demonstrate blockchain's dual promise of enhancing transparency and maintaining confidentiality—a balance that is demanded of contemporary governance. Sectoral requirements contribute to the intricacies of a balance between secrecy and transparency. Convergence of blockchain and IoT in South Korean agriculture ensures farm-to-market traceability while farmer data is safeguarded (Choi & Luo, 2019). Healthcare, however, poses unique challenges: Estonia's sharing of health information through blockchain is opposed to Japan's hesitancy based on cultural preferences for centralized decision-making (Fu & Zhu, 2019). These variations are indicative of the role of contextual determinants—e.g., institutional trust and regulatory frameworks—on blockchain effectiveness. To show, for example, the EU's General Data Protection Regulation (GDPR) is at odds with blockchain's immutability, with innovations like "chameleon hashes" in France to accommodate tamperable data alterations (Merlec et al., 2021). In contrast, China's governments reorient blockchain for uses in surveillance, citing how patterns of governance dictate technological application (Kshetri, 2017). Blockchain architecture also has trade-offs. Decentralized and open public blockchains like Ethereum trade openness and decentralization off against scalability and energy efficiency (Ktari et al., 2024). Bitcoin's PoW consensus is energy expensive but secure—a downside addressed by Ethereum switching to PoS in 2023, which reduced energy usage by 99.9% (Min, 2021). Private blockchains such as Hyperledger are centralised and private at the cost of decentralisation and create the "technological lock-in" (Vergne, 2020). Hybrid models such as VeChain's proof-of-authority are attempting to find the middle ground but need to be calibrated correctly so that centralisation does not happen (Sheel & Nath, 2019). These are the kinds of details reflective of the balance between governance goals and blockchain design. The review also exposes methodological weaknesses in the current literature. More than 60% of research was based on theoretical frameworks or case studies, such as the blockchain court pilot of Dubai, that provided deep insights but narrow generalizability (Mahula et al., 2024). Quantitative research, although limited, tended to be plagued by small sample sizes—a 2022 survey of 12 government agencies, for instance, furnished initial evidence of the cost-saving prospects of blockchain but lacked statistical soundness (Grody, 2018). Geographic bias also skewed evidence with 65% of the research conducted in Europe and North America and being region-blind to locations in sub-Saharan Africa where blockchain can bridge land-right gaps (Soner et al., 2021). Temporal constraint bias was also present with most of the research conducted before 2023, without innovations such as quantum-resistant blockchains (F. Wang et al., 2024). In spite of these constraints, grey literature such as World Bank reports reduced publication bias and enabled synthesis (Ning et al., 2021). Their ethical implications cannot be disregarded. Algorithmic bias in West Virginia's blockchain voting pilot put into doubt the exclusion of marginalized communities (Bennett & Uche MTech, 2023), echoing caution against "trustlessness" in public systems. Similarly, developer-funded research consistently oversold blockchain's benefits while minimising its costs, as with IBM's Hyperledger evaluations (Renwick & Gleasure, 2021). Such biases emphasize the merit of independent, interdisciplinary research in providing equitable outcomes. Practically, blockchain potential is more than transparency and protection. Indonesia's blockchain-based identity systems enhance social services with increased efficiency while also being compliant at the national level with privacy

legislation (Fathiyana et al., 2022). Ghana's health insurance program in cloud-blockchain ensures financial safety by reducing fraud (Amponsah et al., 2022). Scalability, nevertheless, is an issue. While successful on a local scale, South Korea's agricultural blockchain struggles to interoperate with legacy systems—a challenge mirrored in Malaysia's manufacturing sector (Mubarik et al., 2020). Policymakers must prioritize interoperability standards, such as the EU's European Blockchain Services Infrastructure (EBSI), to enable seamless cross-sector adoption (Shi et al., 2024). Three priority needs of future research are. Firstly, longitudinal studies would have to track blockchain influences on society for decades but particularly on healthcare and real estate management (Kassen, 2024). Secondly, regional inclusion must be made a priority: boosting research in Arabic can help address MENA region knowledge gaps (Aliu et al., 2025). Finally, technological advancement must be aimed at energy-efficient consensus algorithms like Algorand's proof of stake (PoS) and AI-blockchain hybrids, in order to combat algorithmic discrimination (Mishra et al., 2024). To exemplify, explainable AI systems may enhance blockchain voting system transparency, which ensures accountability and fairness (Fan et al., 2024). In simple words, blockchain is a data management model of governance with means of maintaining openness and confidentiality. Estonia's health records, Georgia's registry of real property, and countless other successful projects demonstrate how this can cement confidence and efficacy. However, issues like power usage, regulation complexity, and ethics risk remain. Governments have to make blockchain attain its utmost possible potential for the development of just, human-centric systems of governance by embracing adaptation policies, collaborative interagency interactions, and engagement in design processes. As (Kassen, 2025) aptly suggests, the worth of blockchain is neither in its technology but in its potential to transform power relationships—a prospect that requires ambition and prudence.

Implications for Smart City Governance and Data Management

The implications of the systematic review can also be observed in the field of smart city governance and data management, where digital technology has an important role in mediating the relationship between public institutions, smart cities, and citizens. Blockchain technology, rather than being a technological advancement, represents a governance logic, which has the potential to transform the way in which smart city ecosystems operate, including issues of authority, trust, and accountability.

1. Governance Transformation in Smart City Ecosystems

The application of blockchain technology in smart city ecosystems has the potential to bring about a gradual transformation from a centralized platform-based governance approach towards a decentralized governance approach. Governance in smart cities evolves from a focus on the role of the city to a multi-actor governance approach, which involves different actors, including citizens. The transformation in smart city governance is in line with the development of new governance, which includes the development of new governance concepts such as co-production, co-regulation, and co-responsibility in smart cities. The application of smart contracts can further add value to the transformation in smart city governance, which includes the streamlining of regulatory compliance, procurement, and service level agreements.

2. Balancing Transparency and Privacy in Urban Data Environments

In smart cities, there is no end to the collection of data from various sources. As a result, there is often a clash between transparency and privacy. In this regard, the literature reviewed indicated that blockchain technology has provided a more contextual solution to this problem through the use of selective transparency. Through the use of various cryptographic techniques, including zero-knowledge proofs, blockchain technology has provided a way of verifying data without necessarily exposing the data. In smart cities, there is often a clash between transparency and privacy due to the use of data from various domains that often compromise individual or infrastructure security.

3. Hybrid Data Architectures for Scalable Smart City Systems

From a data management perspective, the literature reviewed indicated that there is a clear implication that smart cities require a hybrid data architecture. This is due to the high velocity of data in smart cities. In this regard, it is not possible to store data on a blockchain. However, blockchain technology has provided a way of solving this problem.

4. Citizen-Centered Identity Management and Urban Trust

The adoption of self-sovereign identity management (SSI) is a paradigm shift in the management of our identities as citizens on the internet. Using blockchain, citizens can be empowered to own their credentials, and services

PILAR Nusa Mandiri: Journal of Computing and Information System
Vol. 22, No. 1 March 2026 | DOI: 10.33480/pilar.v22i1.8254

can still be provided to verify the credentials. The adoption of this approach can help build trust in urban centers because it eliminates the issue of one-sided data hoarding and can change the perception of urban centers as data holders to that of issuers of credentials. However, this approach needs to be considered in the context of how to ensure that this technology does not further widen the gap between the disadvantaged.

5. Interoperability Across Urban Systems and Data Silos

Another challenge that has hindered the successful implementation of smart cities has been the fragmented nature of the data in urban centers. According to the review, blockchain can help improve the interoperability between various urban systems, considering that they have different data sets, through secure data exchange, provided that standardized data models are used in the process. This interoperability can help improve the efficiency of the services provided in the various urban systems, including energy, transportation, and waste management, among others, through better forecasting and planning.

6. Regulatory and Ethical Implications for Smart City Governance

The adoption of blockchain technology in urban centers also has several implications on the regulatory environment in smart city governance. For example, the current legislation may not provide adequate provisions regarding algorithmic governance, smart contracts, and decentralized authentication. Urban centers also need to consider the issue of ethics in smart city governance, including issues of data concentration, algorithmic bias, and unequal access to digital technologies. Building capacity in urban centers is important in realizing the value of blockchain innovation.

CONCLUSION

This systematic review explores the way blockchain technology is changing government data management, transparency, and privacy by examining 49 studies published between 2016 and 2025 in peer-reviewed journals. The analysis of existing literature suggests that blockchain technology improves traceability, evidence of tamper attempts, and auditability in government data management while maintaining privacy and confidentiality by design. However, rather than eliminating the trade-offs between transparency and privacy, blockchain technology has redefined them by incorporating security features that depend on its design. Three analytical patterns were observed in the thematic analysis of existing literature: The technological mediation pattern, which describes the use of cryptography tools as a bridge between transparency and privacy; The governance and architecture alignment pattern, which describes the alignment of blockchain technology with varying institutional logics and regulatory frameworks; and The context dependency pattern, which describes the significant differences in outcomes depending on institutional capacity and regulatory maturity in each context. The review also identifies some gaps in the current literature. A significant portion of the literature relies on conceptual models or pilot studies, which makes it difficult for the results to be generalized beyond the particular context in which they were conducted. There is also a lack of large-scale and long-term empirical research, and ongoing research into institutional trust. Furthermore, it should be noted that the literature is dominated by research from European and Asian countries, which makes it difficult for the results to be generalized beyond these regions. Overall, it should be noted that the results of the current literature should be taken with caution. The recommendations for policymakers are quite clear: in order for blockchain technology to be successfully integrated into government systems, it should be accompanied by flexible regulatory experimentation, the development of interoperability standards, and critical examination of the process of reaching consensus in the context of sustainability objectives. Moreover, it should be noted that the results of the current literature also highlight the importance of inclusive system development and institutional oversight in order to avoid lock-in and digital exclusion. It should be noted that sector-specific strategies appear to be more in line with what is found in the data compared to general deployment strategies.

Future research would benefit from long-term research into governance, comparisons between regions, and quantitative research into the cost-benefit ratio of blockchain infrastructures. Furthermore, it would be interesting for future research to examine further the benefits of energy efficiency in the process of reaching consensus, quantum-resistant cryptography, and artificial intelligence and blockchain integration in order to better understand the development of the technology in the context of digital governance systems. In conclusion, it should be noted that blockchain technology should not be seen as a panacea for transparency and confidentiality in the context of public governance systems. Instead, it should be seen as a dynamic tool for governance whose success depends on the level of alignment between technical, regulatory, and institutional systems. Its benefits should be seen in the context of

trust redistribution and formalization, depending on the context in which it is applied and how it is applied.

AUTHOR CONTRIBUTIONS

Author 1 made the primary and leading contribution to this study. This author conceived the research idea, designed the overall conceptual and methodological framework, formulated the research objectives and questions, and supervised all stages of the research process. Author 1 also led the interpretation of findings, ensured methodological rigor, and conducted the final critical review of the manuscript for intellectual depth, coherence, and scientific quality. contributed to the systematic literature search, study screening and selection, data extraction, and preliminary thematic organization of the included studies. This author also assisted in the development of analytical tables and supported the synthesis of empirical evidence.
Author 2 contributed to data synthesis, thematic analysis, and interpretation of results. This author supported the refinement of the discussion section, assisted in structuring the results, and contributed to manuscript editing to improve clarity, consistency, and academic presentation.
All authors participated in drafting the manuscript, revising it critically for important intellectual content, and approving the final version for submission. All authors agree to be accountable for all aspects of the work.

CONFLICT OF INTEREST STATEMENT

All authors disclose no financial, personal, or professional interests that might prejudice the study or its results, implications, or views. Based on study results, choices and suggestions are made.

FUNDING REPORT

The authors say no government, commercial, or other organization financed this study.

ETHICS APPROVAL STATEMENT

The authors argue this study does not require ethical approval since there were no human or animal experiments.

REFERENCE

Aliu, J., Oke, A. E., & Ehiosun, L. U. (2025). Distributed ledger technology integration in Nigerian construction industry: key drivers. *International Journal of Building Pathology and Adaptation*, *43*(7), 1706–1724. https://doi.org/10.1108/ijbpa-02-2024-0044

Amponsah, A. A., Adekoya, A. F., & Weyori, B. A. (2022). Improving the Financial Security of National Health Insurance using Cloud-Based Blockchain Technology Application. *International Journal of Information Management Data Insights*, *2*(1), 100081. https://doi.org/10.1016/j.jjimei.2022.100081

Azzam, F., Jaber, M., Saies, A., Kirresh, T., Awadallah, R., Karakra, A., Barghouthi, H., & Amarneh, S. (2023). The Use of Blockchain Technology and OCR in E-Government for Document Management: Inbound Invoice Management as an Example. *Applied Sciences, 13*(14), 8463. https://doi.org/10.3390/app13148463

Banabilah, S., Aloqaily, M., Alsayed, E., Malik, N., & Jararweh, Y. (2022). Federated learning review: Fundamentals, enabling technologies, and future applications. *Information Processing & Management*, *59*(6), 103061. https://doi.org/10.1016/j.ipm.2022.103061

Benítez-Martínez, F. L., Hurtado-Torres, M. V., & Romero-Frías, E. (2021). A neural blockchain for a tokenizable e-Participation model. *Neurocomputing*, *423*, 703–712. https://doi.org/10.1016/j.neucom.2020.03.116

Bennett, B., & Uche MTech, C. (2023). A FRAMEWORK FOR BIRTH DATA REGISTRATION AND VERIFICATION USING SMART CONTRACTS, PUBLIC KEY ENCRYPTION, AND NATIONAL IDENTIFICATION NUMBER (NIN). Retrieved from http://irepo.futminna.edu.ng:8080/jspui/handle/123456789/19712

Benouachane, H. (2022). Artificial Intelligence in Social Security: Opportunities and Challenges. *The Journal of Social Policy Studies, 20*(3), 407–418. https://doi.org/10.17323/727-0634-2022-20-3-407-418

Carter, G., Chevellereau, B., Shahriar, H., & Sneha, S. (2020). OpenPharma Blockchain on FHIR: An Interoperable Solution for Read-Only Health Records Exchange through Blockchain and Biometrics. *Blockchain in Healthcare Today*, *3*, 1-10. https://doi.org/10.30953/bhty.v3.120

Chen, J., Lv, Z., & Song, H. (2019). Design of personnel big data management system based on blockchain. *Future Generation Computer Systems*, *101*, 1122–1129. https://doi.org/10.1016/j.future.2019.07.037

CHEN, Y., HAO, Y., YI, Z., GUO, X., & XU, C. (2024). BCS: Blockchain-based Ciphertext Storage

Scheme Supporting Data Hierarchical Management. *Journal of Information Science and Engineering, 40*(1), 1-26. https://doi.org/10.6688/JISE.202401_40(1).0001

Choi, T. M., & Luo, S. (2019). Data quality challenges for sustainable fashion supply chain operations in emerging markets: Roles of blockchain, government sponsors and environment taxes. *Transportation Research Part E: Logistics and Transportation Review*, *131*, 139–152. https://doi.org/10.1016/j.tre.2019.09.019

Elisa, N., Yang, L., Chao, F., & Cao, Y. (2018). A framework of blockchain-based secure and privacy-preserving E-government system. *Wireless Networks, 29*(3), 1005–1015. https://doi.org/10.1007/s11276-018-1883-0

Fan, J., Wang, Q., & Wang, Y. (2024). The Impact of Blockchain on the Administrative Efficiency of Provincial Governments Based on the Data Envelopment Analysis–Tobit Model. *Sustainability, 16*(7), 2909. https://doi.org/10.3390/su16072909

Fathiyana, R. Z., Yutia, S. N., & Hidayat, D. J. (2022). Prototype of Integrated National Identity Storage Security System in Indonesia using Blockchain Technology. *JOIV : International Journal on Informatics Visualization*, *6*(1), 109–116. doi:10.30630/joiv.6.1.877

Fu, Y., & Zhu, J. (2019). Operation Mechanism for G2B System Based on Blockchain. *Tehnički Vjesnik*, *26*(6), 1841–1852. doi:10.17559/TV-20190722100223

Ghazali, R., Ali, F. H. M., Bakar, H. A., Ahmad, M. N., Haron, N. S., Omar, A. H., & Ahmadian, A. (2021). Blockchain for record-keeping and data verifying: proof of concept. *Multimedia Tools and Applications 2021 81:25*, *81*(25), 36587–36605. doi:10.1007/s11042-021-11336-7

Grody, A. D. (2018). Rebuilding financial industry infrastructure.

Kapsoulis, N., Psychas, A., Litke, A., & Varvarigou, T. (2024). Blockchain privacy: Fundamental aspects and challenges for the future Internet data sharing. *IET Blockchain*, *4*(2), 152–168. doi:10.1049/blc2.12058

Kassen, M. (2024). Blockchain and public service delivery: a lifetime cross-referenced model for e-government. *Enterprise Information Systems*, *18*(4). doi:10.1080/17517575.2024.2317175

Kassen, M. (2025). Blockchain and digital governance: Decentralization of decision making policy. *Review of Policy Research*, *42*(1), 95–121. doi:10.1111/ropr.12585

Khan, M., Imtiaz, S., Parvaiz, G. S., Hussain, A., & Bae, J. (2021). Integration of Internet-of-Things with Blockchain Technology to Enhance Humanitarian Logistics Performance. *IEEE Access*, *9*, 25422–25436. doi:10.1109/ACCESS.2021.3054771

Krysovatyy, A., Desyatnyuk, O., & Ptashchenko, O. (2024). Digital Innovations and their Ramifications for Financial and State Security. *AFRICAN JOURNAL OF APPLIED RESEARCH*, *10*(1), 431–441. doi:10.26437/ajar.v10i1.713

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy*, *41*(10), 1027–1038. doi:10.1016/j.telpol.2017.09.003

Ktari, J., Frikha, T., Hamdi, M., & Hamam, H. (2024). Enhancing Blockchain Consensus with FPGA: Accelerating Implementation for Efficiency. *IEEE Access*, *12*, 44773–44785. doi:10.1109/ACCESS.2024.3379374

Lemieux, V. L., Rowell, C., Seidel, M. D. L., & Woo, C. C. (2020). Caught in the middle? Strategic information governance disruptions in the era of blockchain and distributed trust. *Records Management Journal*, *30*(3), 301–324. https://doi.org/10.1108/rmj-09-2019-0048

Li, R., & Wan, Y. (2021). Analysis of the Negative Relationship between Blockchain Application and Corporate Performance. *Mobile Information Systems*, *2021*(1), 1–18. https://doi.org/10.1155/2021/9912241

Mahula, S., Tan, E., Crompvoets, J., & Timmers, P. (2024). What motivates public sector organisations to use blockchain?. *International Journal of Public Sector Management*, *38*(1), 118–138. https://doi.org/10.1108/ijpsm-12-2023-0361

Malik, V., Mittal, R., Mavaluru, D., Narapureddy, B. R., Goyal, S. B., Martin, R. J., Srinivasan, K., & Mittal, A. (2023). Building a Secure Platform for Digital Governance Interoperability and Data Exchange Using Blockchain and Deep Learning-Based Frameworks. *IEEE Access, 11*, 70110–70131. https://doi.org/10.1109/access.2023.3293529

Merlec, M. M., Lee, Y. K., Hong, S. P., & In, H. P. (2021). A Smart Contract-Based Dynamic Consent Management System for Personal Data Usage under GDPR. *Sensors, 21*(23), 7994. https://doi.org/10.3390/s21237994

Min, Y. A. (2021). The Modification of pBFT Algorithm to Increase Network Operations Efficiency in Private Blockchains. *Applied Sciences, 11*(14), 6313. https://doi.org/10.3390/app11146313

Mishra, R., Kr Singh, R., Daim, T. U., Fosso Wamba, S., & Song, M. (2024). Integrated usage of artificial intelligence, blockchain and the internet of things in logistics for decarbonization through paradox lens. *Transportation Research Part E: Logistics and Transportation Review*, *189*, 103684. https://doi.org/10.1016/j.tre.2024.103684

Morrow, M. J., & Zarrebini, M. (2019). Blockchain and the Tokenization of the Individual: Societal Implications. *Future Internet, 11*(10), 220. https://doi.org/10.3390/fi11100220

Mubarik, M., Rasi, R. Z. binti R. M., & Mubarak, M. F. (2020). Fostering Supply Chain Integration through Blockchain Technology: A Study of Malaysian Manufacturing Sector. *International Journal of Management and Sustainability, 9*(3), 135–147. https://doi.org/10.18488/journal.11.2020.93.135.147

Ning, X., Ramirez, R., & Khuntia, J. (2021). Blockchain-enabled government efficiency and impartiality: using blockchain for targeted poverty alleviation in a city in China. *Information Technology for Development*, *27*(3), 599–616. https://doi.org/10.1080/02681102.2021.1925619

Potestà, G. (2021). Sustainable Development of Arabian Gulf Cities. *The International Journal of Social Sustainability in Economic, Social, and Cultural Context*, *17*(2), 99–113. https://doi.org/10.18848/2325-1115/cgp/v17i02/99-113

Premkumar, N., & Santhosh, R. (2023). Pelican optimization algorithm with blockchain for secure load balancing in fog computing. *Multimedia Tools and Applications, 83*(18), 53417–53439. https://doi.org/10.1007/s11042-023-17632-8

Renwick, R., & Gleasure, R. (2021). Those who control the code control the rules: How different perspectives of privacy are being written into the code of blockchain systems. *Journal of Information Technology*, *36*(1), 16–38. https://doi.org/10.1177/0268396220944406

Sheel, A., & Nath, V. (2019). Effect of blockchain technology adoption on supply chain adaptability, agility, alignment and performance. *Management Research Review, 42*(12), 1353–1374. https://doi.org/10.1108/mrr-12-2018-0490

Shi, L., Zhou, Y., Wang, W., Wang, J., Bai, Y., Peng, C., Chen, D., & Wang, Z. (2024). A Cross-Chain Mechanism for Agricultural Engineering Document Management Blockchain in the Context of Big Data. *Big Data Research, 36*, 100459. https://doi.org/10.1016/j.bdr.2024.100459

Soner, S., Litoriya, R., & Pandey, P. (2021). Exploring Blockchain and Smart Contract Technology for Reliable and Secure Land Registration and Record Management. *Wireless Personal Communications, 121*(4), 2495–2509. https://doi.org/10.1007/s11277-021-08833-1

Sotoudehnia, M. (2021). 'Making blockchain real': regulatory discourses of blockchains as a smart, civic service. *Regional Studies*, *55*(12), 1857–1867. https://doi.org/10.1080/00343404.2021.1882671

Sun, M., & Zhang, J. (2020). Research on the application of block chain big data platform in the construction of new smart city for low carbon emission and green environment. *Computer Communications*, *149*, 332–342. https://doi.org/10.1016/j.comcom.2019.10.031

Sung, C. S., & Park, J. Y. (2021). Understanding of blockchain-based identity management system adoption in the public sector. *Journal of Enterprise Information Management*, *34*(5), 1481–1505. https://doi.org/10.1108/jeim-12-2020-0532

Thakur, V., Doja, M. N., Dwivedi, Y. K., Ahmad, T., & Khadanga, G. (2020). Land records on Blockchain for implementation of Land Titling in India. *International Journal of Information Management*, *52*, 101940. https://doi.org/10.1016/j.ijinfomgt.2019.04.013

Tseng, J. H., Liao, Y. C., Chong, B., & Liao, S. W. (2018). Governance on the Drug Supply Chain via Gcoin Blockchain. *International Journal of Environmental Research and Public Health, 15*(6), 1055. https://doi.org/10.3390/ijerph15061055

Vergne, J. P. (2020). Decentralized vs. Distributed Organization: Blockchain, Machine Learning and the Future of the Digital Platform. *Organization Theory*, *1*(4). https://doi.org/10.1177/2631787720977052

Wang, F., Gai, Y., & Zhang, H. (2024). Blockchain user digital identity big data and information security process protection based on network trust. *Journal of King Saud University - Computer and Information Sciences*, *36*(4), 102031. https://doi.org/10.1016/j.jksuci.2024.102031

PILAR Nusa Mandiri: Journal of Computing and Information System
Vol. 22, No. 1 March 2026 | DOI: 10.33480/pilar.v22i1.8254

Wang, P., Wang, X., Shen, Y., Wang, J., & Xiong, X. (2023). PBFT optimization algorithm based on community contributions. *Mathematical Biosciences and Engineering, 20*(6), 10200–10222. https://doi.org/10.3934/mbe.2023447

Zhang, X. (2022). The use of ethereum blockchain using internet of things technology in information and fund management of financial poverty alleviation system. *International Journal of System Assurance Engineering and Management, 13*(S3), 1205–1215. https://doi.org/10.1007/s13198-022-01644-y