Secure Data Sharing Using Blockchain Technology: A Systematic Literature Review

Azman Azmi[1], Farashazillah Yahya[2]*, Nur Afrina Azman[3], Hazlina Jalil[4]
Faculty of Computing and Informatics, Universiti Malaysia Sabah, Malaysia[1, 2]
School of Mathematical, Physical and Computational Sciences, University of Reading, United Kingdom[3]
The Southeast Johor Development Authority (KEJORA), Bandar Penawar, Johor, Malaysia[4]

***Abstract*—Data sharing security is currently one of the crucial parts in e-government systems. Although blockchain, a type of Distributed Ledger Technology (DLT), has been increasingly applied to enhance secure data exchange, there is a significant lack of studies focusing on the specific security factors that underpin its implementation in e-government contexts. Defining and understanding these factors is crucial for the successful integration of blockchain into public data infrastructures. This study addresses this research gap through a Systematic Literature Review (SLR) guided by the PRISMA 2020 framework. A total of 511 articles were retrieved from five major databases, and 103 were selected and systematically reviewed using the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 approach. While the majority of studies emphasised privacy, integrity, and transparency, other critical security factors such as scalability, availability, governance, and decentralisation remain comparatively underexplored. The theory of blockchain-based data sharing security factors was developed as a reference. The article wraps up the discussion by highlighting nine security factors in data sharing using blockchain in e-government for future investigation.**

Keywords*—Blockchain; Distributed Ledger Technology (DLT); data sharing security; e-government; Systematic Literature Review (SLR); PRISMA 2020

I. Introduction

In the era of emerging digital technologies, governments around the world are increasingly adopting technology to improve the accessibility, transparency, and efficiency of public administration using a transformative methodology called electronic government (e-government). A key element of e-government is the secure and seamless exchange of data among various government agencies and citizens. However, traditional data-sharing methods are often plagued by challenges related to trust involving security and privacy, which can hinder the complete effectiveness of e-government initiatives. [1], [2].

Data sharing serves as the cornerstone of e-government, enabling the efficient flow of information between government entities and citizens to ensure streamlined service delivery. However, digital disruption has introduced significant challenges in maintaining information security and privacy. Traditional methods of data sharing have increased the risk of cybersecurity. These attacks include vulnerability attack, data breach, user account compromise and malicious attack. This will further trigger the system safety and reliability issue. [1], [3].

The Malaysia Central Data Sharing platform (MyGDX), provided by the Digital Department of Malaysia, is the most used platform among government agencies. The trend of data sharing among government agencies on this platform showed an increase in transactions every year. The number of data sharing transactions recorded from the beginning of the data sharing exchange in 2018 to 26 May 2024 was recorded at 621,824 transactions. However, a total of 4,117,202 data sharing transactions were recorded by the 12th of May 2025 [4]. These statistics express a growth of 3,485,378 transactions from May of 2024 to May of 2025 alone. A breach involving such a large dataset will pose significant risk due to the scale and critical nature of the information.

According to Malaysia Computer Emergency Response Team (MyCERT), Cyber General Incident Classification statistics – January to April 2025[5]. There were 2,291 incidents received by Cyber999 Incident Response Centre, compared to the 1,550 incidents received in Q4 2024. This indicates that there is a 7% increase in incidents in the previous quarter. Personal identifiable information (PII) from national databases, such as identity numbers, addresses, and financial data, is commonly involved in high-profile attacks, according to MyCERT.

This research aims to comprehensively and systematically review the literature as well as synthesise current work on blockchain-based data sharing in e-government systems. The main focus is to identify the key factors for secure data sharing. The review aims to analyse the existing frameworks and models proposed for application of blockchain in electronic government, assess the effectiveness of these approaches in improving data sharing practices, and stress the gaps in the recent literature. Ultimately, this review aims to deliver a clear understanding of the latest use of blockchain-based data sharing within e-government systems and to identify prospective investigations in this evolving area.

II. Study Background

A. Data Sharing

Data sharing is essential to promote collaboration and innovation in various domains. The integration of technologies can improve the privacy and security of data sharing, addressing concerns related to the issue and challenges of data security.

The term data sharing refers to the movement of information between different systems and entities or across international borders. It is crucial for decision makers, resource optimisation,

*Corresponding Author

and improving information utilisation. [6]. In the public sector, data sharing is vital for addressing interoperability challenges, such as collaboration between government agencies and seamless information exchange. The process involves the exchange of information and knowledge between organisations through their business processes [7], [8].

Both definitions highlighted that data sharing is important to parties which benefit from data sharing. The United Kingdom Information Commissioner's Office highlights the importance of responsible data sharing, stating: "When you get data protection right, it sends a strong message to your customers – it lets them know that you value and care for their information and that you are more likely to keep it safe and not share it inappropriately"[9]. This statement further reinforces the critical role of trust, ethical practices, and robust security measures in data sharing processes, ensuring that organisations handle information responsibly while maximising its potential for social and organisational benefits.

B. Data Sharing Security

Data sharing security is a critical aspect of modern information systems, ensuring that data is shared between entities in a way that protects its confidentiality, integrity, and availability. The fundamental model used in information security is the CIA triad, which stands for confidentiality, integrity, and availability [10]. This model serves as a reference framework for agencies to protect delicate data and ensure that information systems are secure. Each component of the triad addresses a specific aspect of security and together provides a comprehensive approach to safeguarding information.

Based on the NIST Cyber Security Framework 2.0 [11], Data security refers to the consistent management of data in a proper manner within the organization and protects all the risk of providing trust through confidentiality, integrity, and availability of information in all data conditions, whether the data at rest, data in transit, data in use and backups of data are created, protected, maintained, and tested.

1) Confidentiality: The NIST refers to the term confidentiality as the preservation of authorised restrictions on information access and disclosure, including means to protect personal privacy and proprietary information...[12]. Confidentiality involves ensuring reachability of data by authorised personnel. Sensitive data needs to be secure from data leaks and breaches.

2) Integrity: Integrity was demarcated by the NIST as protection for data from being improperly altered, modified or demolished by protecting the information's originality and legitimacy [11]. The term integrity also refers to the precision and fullness of data. The integrity ensures information is not changed in unauthorised ways, while at the same time, providing the reliability and trustworthiness of the data [12].

3) Availability: Availability guarantees that resources and information are available to authorised users when needed. It is essential for upholding the practicality and usability of information systems. The NIST defines availability as "Ensuring timely and reliable access to and use of information…"[12].

C. Blockchain Technology Security

Blockchain Technology or Distributed Ledger Technology is one of the emerging technologies of Industrial Revolution 4.0, which is used in data security. Introduced by Nakamoto, Blockchain Technology offers a decentralised and secure method for recording transactions. Blockchain technology is characterised by the ability to maintain a distributed ledger that is immutable, transparent and resistant to tampering [13].

In blockchain technology, the new transaction created by a user will be broadcast to the blockchain network using a P2P connection. Then, the node in the network will validate the transaction using a consensus mechanism like Proof of Work (PoW). Validated transactions are grouped in a block. The block will be linked to the chain using a cryptographic hash. The ledger will be updated to complete the transaction as shown in Fig. 1.

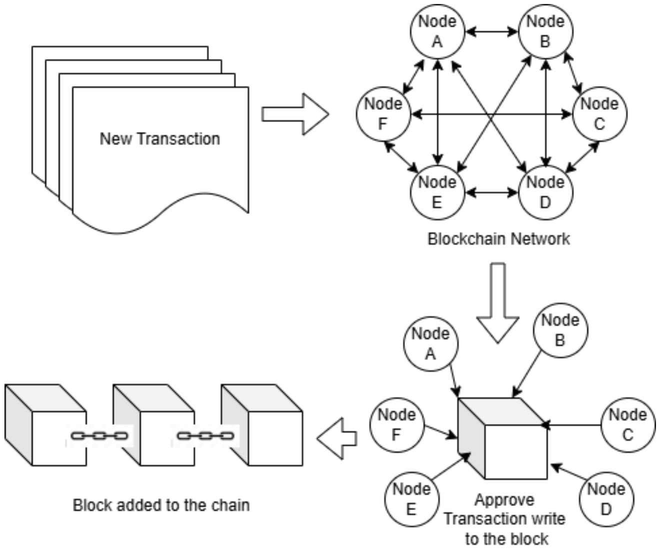

Fig. 1. How blockchain works.

D. E-Government System Data Security

The term, electronic government (e-government), is defined by [1] as the application of ICT to digitalise government services for the public, enterprises, and government agencies. The objectives of having an e-government system include reducing bureaucracy, increasing transparency, and ensuring secure and efficient service delivery. [1], [7], [14], [15]. According to [16], current data-sharing practices in e-government systems face several challenges that hinder effectiveness and security.

The governing policy and act are the most important items to be complied with for the e-government data sharing security in government agencies. In 2021, the Malaysia Administrative and Modernisation dan Planning Unit (MAMPU) released the Policy for Public Sector Data Sharing. This is used to govern the cross-organisation data sharing to improve services towards data-driven government [17]. Recently, in February of 2025, the establishment of the National Data Sharing Committee led by the Director General of the National Digital Department has aligned with the passing of the bill of Data Sharing Act 2025 (Act 864) by providing control to the public sector regarding data sharing processes [18].

III. Methodology

Data Sharing, security, and e-government applications have a vast amount of literature in general. Many academic papers and government reports have discussed Blockchain topics. An extensive search has been made, and the current development studies published between the years 2014 and 2024 have been discussed in this paper. The selection of the publication article aligns with the issues related to the security of data sharing, specifically involving the e-government system. These issues have been discussed, debated, and reported at international and national levels. This paper discusses the selected papers from established journals, conference papers, and proceedings.

The PRISMA 2020 (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) protocol is a widely recognised and standardised framework used to ensure transparency, rigour, and reproducibility in conducting and reporting systematic reviews [19]. For this systematic literature review on blockchain-based data sharing in e-government systems, the PRISMA 2020 protocol was meticulously followed to guide the review process. Based on the keywords search, a collection of comprehensive artefacts was gathered. Four phases were involved in searching and selecting the papers: identification, screening, eligibility, and inclusion, as illustrated in Fig. 2.

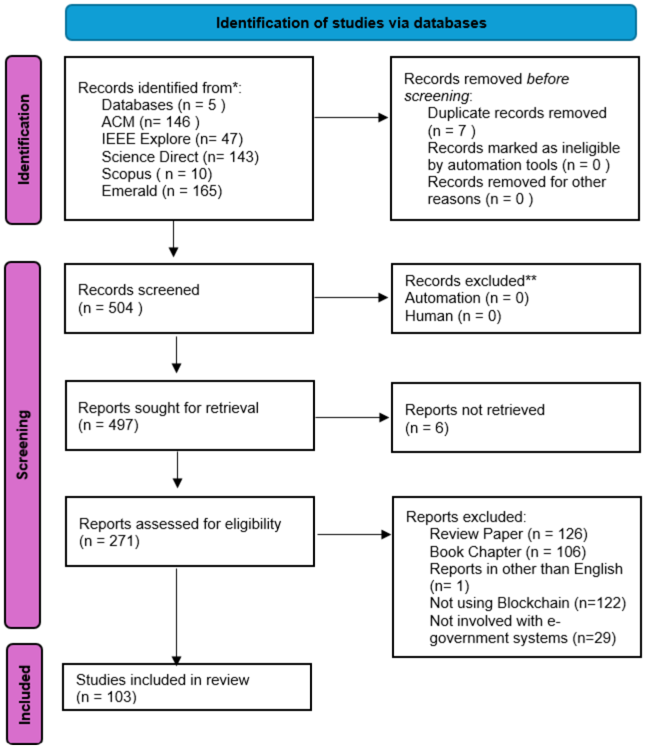
Identification of studies via databases
Identification
Screening
Included
Records identified from*:
Databases (n = 5)
ACM (n= 146)
IEEE Explore (n= 47)
Science Direct (n= 143)
Scopus (n = 10)
Emerald (n = 165)
Records removed *before screening*:
Duplicate records removed (n = 7)
Records marked as ineligible by automation tools (n = 0)
Records removed for other reasons (n = 0)
Records screened
(n = 504)
Records excluded**
Automation (n = 0)
Human (n = 0)
Reports sought for retrieval
(n = 497)
Reports not retrieved
(n = 6)
Reports assessed for eligibility
(n = 271)
Reports excluded:
Review Paper (n = 126)
Book Chapter (n = 106)
Reports in other than English (n= 1)
Not using Blockchain (n=122)
Not involved with e-government systems (n=29)
Studies included in review
(n = 103)

Fig. 2. Review workflow of this systematic review.

By adhering to the PRISMA 2020 protocol, this systematic review ensures a rigorous, transparent, and reproducible process. Ultimately, providing a comprehensive synthesis of the current state of blockchain-based data sharing in e-government systems.

A. Identification of the Key Research Question

Based on the Key research question, the PICOC framework [19] has been used to define and structure research questions and identify the relevant literature. The key elements of the research context are represented in Table I. The context in the comparison in the systematic review is excluded.

TABLE I. PICOC Framework Mapping with Keywords and Synonyms

PICOC	Description	Keyword	Synonym
Population	An industry domain.	government	
Intervention	The methodology, tool, or technology that tackles a certain problem.	data sharing	data exchange
Comparison	The methodology, tool, or technology in which the Intervention is being compared (if appropriate).	Blockchain	DLT
Outcome	Factors of importance to practitioners and/or the results that interposition could produce.	security	-
Context	The context in which the comparison is done.	e-government	digital government

The research questions guiding this systematic literature review are designed based on the PICOC framework to explore the current landscape of blockchain-based data sharing in e-government systems. The PICOC framework keywords used in this research are in Table I. The population used is e-government or digital government, which is the domain of the research. The Intervention for this research is data sharing or data exchange. The comparison of the technology used is blockchain or Distributed Ledger Technology. Finally, the outcome for the keyword used is security. No context specifies for the research keyword, and it is optional based on the approach.

Specifically, the review seeks to answer the following questions:

RQ 1: What is the current trend in blockchain technology for securing data sharing in e-government systems?

RQ 2: What is the current approach and use of blockchain-based data sharing in e-government systems?

RQ 3: What are the data sharing security factors that blockchain technology enhances in e-government systems?

These questions aim to present a comprehensive understanding of how blockchain technology is being leveraged in highlighting the questions of secure data sharing in e-government, while also identifying areas where further investigation is needed.

B. Identification of Relevant Articles

The selection of databases was based on their relevance to the fields of information security, information systems, and public administration, ensuring an inclusive coverage of the literature.

The review began with a comprehensive search strategy across several academic databases such as Scopus, IEEE Xplore, Science Direct, ACM Digital Library and Emerald. The keyword used in the search included a combination of keywords related to "blockchain OR Distributed Ledger Technology", "data sharing OR information sharing", "e-government", and "security." To enhance the exploration and to make sure that related studies were taken, a Boolean operator is used.

C. Selection of the Relevant Articles: Inclusion and Exclusion Criteria

As mentioned earlier, PRISMA 2020 was used to carefully select the relevant articles for this study. Table II shows that the inclusion criteria 1 is the article. The articles show the use of blockchain in data sharing for e-government systems. Inclusion criteria 2 are the improvements made due to blockchain application in government data sharing as shown in the paper. The exclusion criteria set for this review are that the implementation of blockchain is not mentioned in the paper, and papers have redundancies for the research done.

TABLE II. INCLUSION AND EXCLUSION CRITERIA IN REVIEW SELECTION

Criteria	Justification
IC-1: The articles show the use of blockchain in data sharing for e-government systems.	This review inspects related studies on blockchain used for data sharing in government-related systems.
IC-2: The improvements due to blockchain application in government data sharing are shown in the paper	The aim is to convey an indication Important progress of blockchain technology in data sharing and e-government.
EC-1: Implementation of blockchain is not mentioned in the paper.	Papers that only overview blockchain in general often lack focus on data sharing.
EC-2: Paper is redundant for the research done.	Duplicate content is assessed by com paring publication dates and author status for validity.

In the selection phase, the titles and abstracts of the 497 selected articles were read and evaluated manually. Of those, 390 articles were found to be outside the limits of this study, and thus only the remaining 271 articles were taken into account for further analysis. A complete analysis was performed for these 271 articles by carefully inspecting the whole text. This detailed analysis found 168 articles that were not related to this study as they were not relevant to the use of blockchain in data sharing for e-government. Thus, they were also expelled. 103 articles were finalised on the significant publication used for this study, as detailed in Table III.

TABLE III. DISTRIBUTION OF PAPERS BY SOURCES THROUGHOUT THE SCREENING PROCESS

Source	Identification Search	Paper Screening	Eligible Search	Selected for Review
ACM	146	143	44	19
IEEE Xplore	47	46	36	30
Science Direct	143	142	84	27
Scopus	10	8	7	4
Emerald	165	165	100	23
TOTAL	**511**	**504**	**271**	**103**

D. Reporting and Summarising the Results

The first stage was to extract and compile metadata from 271 relevance articles. The metadata consisted of the authors' names, publication title, year of publication, approach used, improved factors, and the security threat problem. These metadata were thoroughly examined using quantitative methods. The purpose of descriptive statistics was to find trends and patterns. Sections IV and V below provide all of these analyses.

IV. RESULTS

A. Trends of Articles Based on PICOC Keywords for 10 Years

The keyword search shown in Fig. 3 shows an upward trend of publications from the year 2016 to 2024. The trend of eligible articles shows the same pattern. The number of articles related to Blockchain approach in data sharing for e-government is expected to increase, as shown in Fig. 3. In 2024, fewer articles were produced as the research was only done until Sept of 2024. There will be more articles published by the end of the year and will increase number of publications, which we believe is an area of further investigation. This will answer Research Question 1 (RQ 1) for What is the current trend in blockchain technology for securing data sharing in e-government systems?

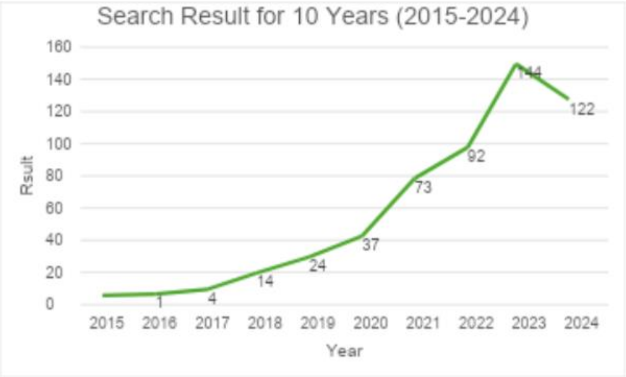

Fig. 3. Trend of article distribution based on 511 articles (Identification Phase).

The findings have shown that evidence of blockchain technology has been widely used to enhance security for data sharing in the e-government. Since 2015, the number of articles published has increased significantly. The number of publications increased by 250% in 2018 from the previous year. Year 2021 has recorded an increase of 36 articles for blockchain-based data sharing compared to 2020, while 92 articles were recorded in 2022. In 2023, 144 articles have been published, which is an increase of 52% from the previous year. The research on the topic began in 2016, which might be influenced by the launch of the Ethereum platform in blockchain technology in 2015 [20].

Based on the distribution of the articles shown in Fig. 4, 103 articles have been identified as eligible to be included in the study. From this, there is only one article which was eligible to be included from 2016. The number of eligible articles increased yearly. However, in 2019, the eligible article was down by 1 article from the year 2018, while 2022 recorded a downtrend of 2 articles from 2021. In certain instances, the paper was excluded due to its failure to address a particular case study. The eligible articles included in 2023 amounted to 29, which is the highest number of articles recorded in a given year. This shows the increment of 12 articles. The number of articles for 2024 is only 14, as the literature cut-off searching date was set to 30 September 2024.

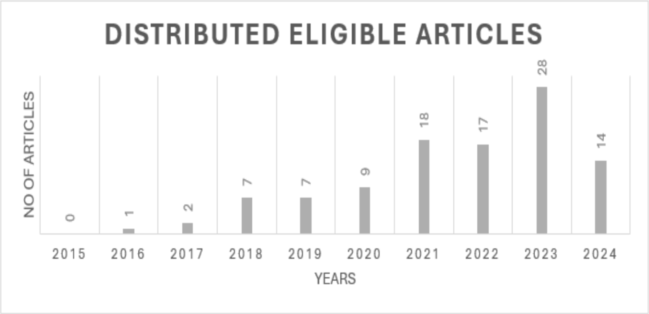

Fig. 4. Distribution of the shortlisted 103 articles based on inclusion and exclusion criteria (Eligibility Phase).

B. State of the Art Blockchain-Based Data Sharing in e-government Systems

The use of blockchain in data sharing has been implemented in several ways to enhance security. RQ 2 What is the current trend and landscape of blockchain-based data sharing in e-government systems in the world? The approach used is governance, adoption, and application. Four (4) articles were focused on the usage of blockchain in enhancing data sharing with compliance with the law and act as General Data Protection Regulation (GDPR), European Timber Regulation and EU's Carbon Border Adjustment Mechanism (CBAM). There is one article for compliance in 2022 and two in 2023, as shown in Fig. 5.

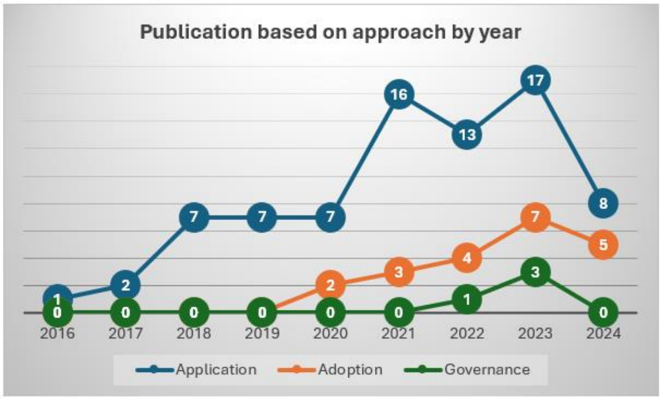

Fig. 5. Trend in publication on approach by year.

The second approach focuses on how organisations adopt blockchain to secure data sharing in e-government. 22 articles researched the acceptance of blockchain security in e-government systems for organisations due to their aptitude to enhance data sharing security. The articles on adoption of blockchain were discovered to begin in 2019 and are increasing every year until 2023, as shown in Fig. 5. In 2024, it is expected to grow as five articles are recorded as of September 2024.

However, the preferred approach to enhance data sharing in e-government data sharing is the application of blockchain in the e-government system. 68 or 56.67% of the eligible articles are on the application of blockchain. Application through integration with existing technology or emerging technologies in one of the four approaches found in this literature. 26 articles used the integration approach in implementing blockchain with IoT, Big Data and cloud computing to enhance the data sharing security. The approach is mostly used for blockchain data sharing security. The trend is static for three years since 2018, and the highest eligible article for application recorded in 2023 is 17, as shown in Fig. 5. In 2024, the number of articles is expected to show 8 articles published and still counting due to the interest of researchers in exploring blockchain technology to secure data sharing in e-government systems continuously.

C. The Landscape of Blockchain-Based Secure Data Sharing Based on Geographical Area and Country

The use of blockchain in the world is expanding from year to year. Currently, 36 countries have been identified in this research to be securing data sharing using blockchain in e-government systems as shown in Fig. 6. China has twelve use cases, which is the highest number of blockchain-based data sharing which covering the implementation in data sharing and big data [21], [22], [23], economic and e-commerce [24], [25], [26]Identity and data management [27], [28], [29], [30], [31] and finally adoption of blockchain technology [32].

There are seven research studies from India. The Indian government used blockchain in the supply chain in government. [33], [34], [35] and aid management [36]. There are use cases in document security which use blockchain data sharing solutions in India. [37], [38] while [39] study how the government accept blockchain technology in the administration.

Estonia recorded five research which is the same as United Arab Emirates (UAE). These countries are focusing on big data and data sharing. [40], [41], blockchain Infrastructure for data sharing [42], [43], [44] and service delivery involving Austria and Australia [45], Utility [46], and services on disaster recovery and real estate [47], [48].

Germany and the Netherlands recorded four studies each. Blockchain is used for monitoring the transparency of the transaction data sharing for agriculture [49], [50], automotive [51], economy [52] and document management and data sharing [8], [41], [53], [54].

The United States (US), United Kingdom (UK), and Nigeria have three research projects in their country. The three countries have data sharing in government healthcare. [44], [55], [56], [57], verification of higher education certificates [58], [59], [60], and identity management [61]. Two studies in the UK are about governance and policy. [62], [63] and property valuation [60].

Malaysia currently has two studies on government data sharing based on blockchain, which is the same as Australia, Finland and Sweden. For the Malaysian case study, blockchain-based data sharing is used for transparency in government aid management. [64] and the adoption in a government agency [15]. Australia is more focused on data sharing for service delivery and smart cities. [45], [65] while Finland studies are recorded as being for ID Management and Economy [40], [66]. In Sweden, studies in this area focus on valued focus thinking [57] and document security [67].

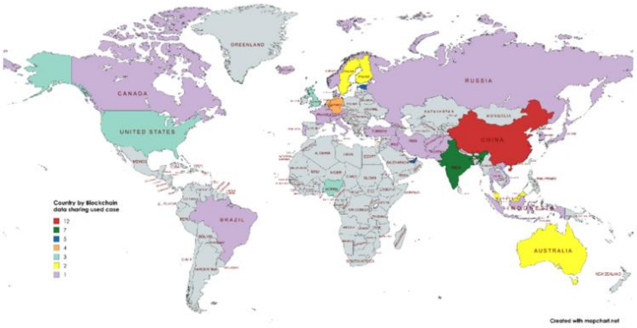

Fig. 6. Blockchain-based data sharing in e-government research heatmap.

22 counties have recorded one publication on data sharing using blockchain. Asian countries like Japan, Vietnam, and Thailand focused on improving data sharing security and trust for decision making in the government system using blockchain. [57], while the publications of Iceland, Indonesia, and South Korea focused on identity security in data sharing [40], [68], [69]. Pakistan and Afghanistan used blockchain in data sharing to secure verification of certification. [14], [70]. Russia and France focused on securing the voting system. [71] While Portugal is securing the data sharing procurement process [72]. On governance, Italy used blockchain in data sharing to comply with the Timber Regulation [73]. Denmark implements a blockchain to secure data sharing in tax management[74]. Iran is using blockchain in cybersecurity [75], Kuwait studies on IoT data sharing [76], and studies in Iraq are using blockchain technology in healthcare [77].

D. *Blockchain-Based Data Sharing Security Factors in e-government Systems*

The security factors are critical aspects in achieving goals in blockchain-based secure data sharing. The security factors involved are extracted from all four approaches in the 103 articles. 77 factors from the articles are structured and present in the word cloud in Fig. 7 and Table IV. This will answer RQ 3 – What are the security factors for blockchain technology used in enhancing the security of data sharing in e-government systems?

This word cloud in Fig. 7 highlights key attributes and factors of data sharing using blockchain technology, emphasising its potential to transform systems based on trust, transparency, and security. The most highlighted security factors are transparency, privacy and integrity, which underscore blockchain's ability to protect sensitive data while ensuring the security processes. The prominent factors of trust, decentralisation, and reliability that reflect blockchain's capacity to eliminate intermediaries, build confidence, and provide reliable systems are also recognised as important factors involved in data sharing security.

The main blockchain concepts, such as immutability and traceability, showcase the technology's ability to ensure data accuracy, prevent tampering, and enable detailed tracking of transactions or assets. In addition, interoperability and scalability factors highlight its adaptability and capacity to handle increasing demand across various systems. In the context of e-government, these attributes align perfectly with the need for secure, efficient, and transparent data-sharing mechanisms, fostering trust between governments and citizens while enhancing operational efficiency.

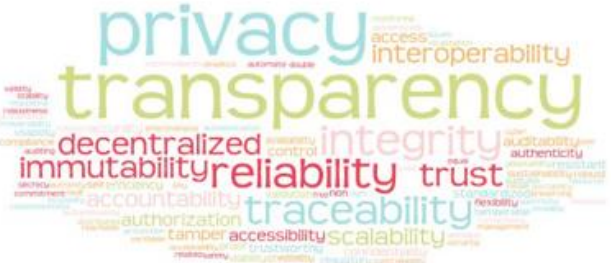

Fig. 7. Word cloud of security factors.

Based on the literature review, 54 characteristics of security factors components have been extracted from 103 articles. The characteristics are based on the NIST Information Security framework, the blockchain security factors and e-government security factors. For the confidentiality factors, Trust between parties, Ensuring Privacy, Data confidentiality, Data ownership, authentication and authorize, secure access control, Identity Security Management and Data sovereignty have been identified in the articles as contributors to the factors.

The integrity factors are the most security factors discussed in blockchain for data sharing, where the subfactors are ensuring or protecting data integrity, single source of truth, trustworthiness of data, verifying authenticity, accuracy and specific, providing validation, reducing fraud, enhancing trust, enhancing accountability, authenticity and reliability of data.

The security factors of using blockchain for data sharing are shown in Fig. 8. The trend shows that integrity recorded 37 articles and is the most secure factor's goal that is achieved in applied blockchain for data sharing in e-government, followed by 33 articles on confidentiality and 27 articles on transparency. The intermediate security factors that attract researchers' attention are 18 articles on interoperability, immutability with 15 articles, auditability with ten articles and decentralize and compliance recorded nine articles for each factor. Availability and Scalability are less focused security factors recorded in six articles and two articles, respectively. Different focus on the security factors shows that priority needs to be established for the factor in securing data sharing using blockchain. The findings reflect the evolving landscape of blockchain security priorities, aligning with the specific needs and challenges of e-government implementations for data sharing.

TABLE IV. INITIAL ALIGNMENT FACTORS FOR BLOCKCHAIN-BASED DATA SHARING SECURITY FACTORS IN E-GOVERNMENT SYSTEMS

Security Factors	**Characteristics**	**Source**
Confidentiality	i. Trust between parties, ii. Ensuring Privacy, iii. Data confidentiality, iv. Data ownership, v. Authenticates, vi. Authorize, vii. Secure access control, viii. Identity Security Management, ix. Data sovereignty	[6], [25], [26], [27], [30], [31], [32], [34], [39], [40], [44], [45], [49], [50], [65], [70], [74], [78], [79], [80], [81], [82], [83], [84], [85], [86], [87], [88], [89], [90], [91], [92]
Integrity	i. Ensuring data Integrity, ii. Protect data Integrity, ii. Single source of truth, iii. Trustworthiness of data, iv. Verify authenticity, v. Accuracy, vi. Providing validation, vii. Reduce fraud, viii. Enhancing trust, ix. Enhanced accountability, x. Authenticity, xi. Reliability source xii. Reliability data, xiii. Specificity	[14], [15], [29], [35], [37], [38], [39], [40], [53], [54], [58], [61], [65], [71], [72], [76], [77], [81], [83], [84], [93], [94], [95], [96], [97], [98], [99], [100], [101], [102], [103], [104], [105], [106], [107], [108]
Availability	i. Enhanced information-sharing across organizations, ii. Make data available, iii. Usability data, iv. Applicability	[24], [56], [80], [83]
Decentralized	i. Enabling distributed power, ii. Decentralisation of property rights, iii. Large-scale data management	[8], [31], [68], [78], [80], [95], [109]
Immutability	i. Reduce the need for trusted third parties, ii. Data protection iii. Tamper-proof record, iv. Resistance to attacks, v. Isolate data vi. block data, vii. Non-temperable	[8], [15], [21], [30], [42], [44], [50], [59], [61], [71], [75], [110], [111], [112], [113]
Transparency	i. Greater transparency, ii. Seamless data sharing among parties, iii. Eliminating intermediaries, iv. Secure transactions, v. Openness of data	[7], [15], [16], [24], [28], [35], [36], [41], [43], [48], [50], [61], [63], [64], [66], [69], [71], [72], [84], [86], [89], [98], [99], [101], [114], [115], [116]
Interoperability	i. Integration data, ii. Harmonise process, iii. Standardisation Integration, iv. Collaboration	[6], [16], [23], [51], [53], [61], [67], [69], [72], [74], [80], [90], [96], [104], [109], [117], [118]
Auditability	i. Transaction can be tracked, ii. Transaction is permanent, iii. Traceability transaction	[8], [31], [32], [50], [63], [73], [80], [88], [112], [113]
Governance	i. Policy, ii. Regulation, iii. Uniformity protocols, iv. Security controls, v. Compliance	[39], [46], [49], [51], [61], [73], [88], [91], [119]

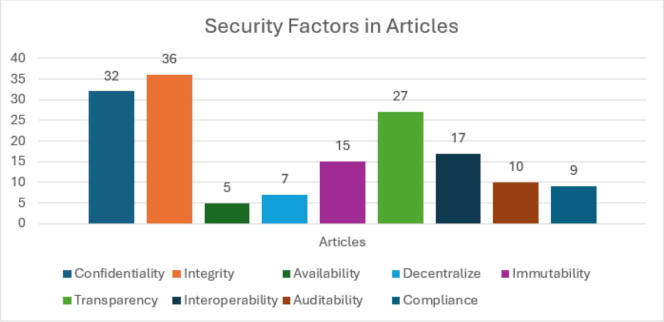

Fig. 8. Security factors.

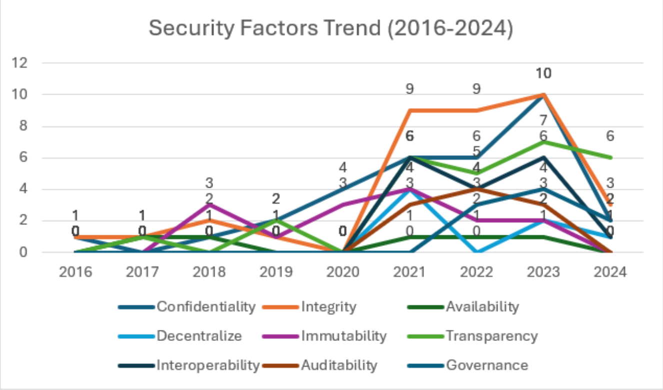

Fig. 9. Security factors trend by year.

The trend in Fig. 9 shows that confidentiality, integrity, transparency, interoperability and compliance factors are trending for the use of blockchain in data sharing security. Integrity factors show the highest trend for three years from 2021 to 2023, followed by confidentiality and transparency. The scalability, availability, immutability, decentralize and show a downtrend while auditability consistently got attention as a security factor that needs to be concentrated on. Based on the pattern, these trends demonstrate the evolving security priorities in blockchain-based data sharing, shaped by emerging challenges and the needs of technological advancements in providing secure data sharing in the domain.

1) Confidentiality: Confidentiality is one of the most important factors that focuses on the government securing data using blockchain technology. Confidentiality concerns can limit the willingness of organisations to share data, as they must ensure data is protected from unauthorised access [120]. Implementing robust confidentiality measures can facilitate data sharing by building trust among stakeholders and ensuring compliance with privacy regulations [120], [121].

2) Availability: In public service, data availability is enhanced through the aggregation of data from various departments into a unified resource catalogue, which supports efficient sharing [122]. The availability of a comprehensive data catalogue allows for better management and sharing of power data, meeting external sharing needs. Public policy plays a dual role as both an enabler and a barrier to data sharing. Contradictions in data availability can arise from legal structures that either facilitate or hinder data linking and sharing, impacting the potential of healthcare data [56].

3) Integrity: Integrity is maintained through rigorous transaction verification processes. Data storage and access transactions involve multiple steps of encryption and signature verification to ensure that data has not been tampered with during transmission [123]. On the other hand, different random parameters are used in generating secret keys, ensuring that data integrity is not compromised by colluding parties [124].

4) Decentralised: Other blockchain technologies' important features for data security are the decentralised factor. Transactions are distributed across the peer-to-peer network

(P2P) by the node and storing the transaction back in the node across the members' network [13]. The distributed ledgers in blockchains are securely synced using a P2P approach, and consensus is made based on smart contracts for the newly added data. Author [125] reported that it is harder to control and alter the data in the distributed network of blockchain because of the consensus built into the technology. Blockchain is a decentralised and trusted authority based on consensus of nodes that take part in the network [126].

5) Immutable: Immutability in blockchain technology has enhanced data sharing security in public service. According to a study [15], immutability is referred to as a fundamental attribute of blockchain. This is one of the important security features of blockchain. Blockchain technology was established as a platform for secure digital transformation technologies in creating immutable records [59], [127].

6) Transparency: Transparency of data had the highest influence on the implementation process in blockchain-based data sharing [41]. Transparency has improved public governance by promoting visibility [7], [64], [66], and enhancing the trust and efficiency of government information sharing [28]. Extended studies to evaluate the effectiveness of blockchain in improving service delivery, transparency, and efficiency in public administration should be done and could involve case studies and comparative analyses with other regions or countries that have successfully implemented blockchain in their e-government initiatives [43].

7) Auditability: Study by [79] assists practitioners and policymakers in implementing auditability using blockchain technology effectively to ensure food safety and improve sustainability in India. Auditability is also a main focus in facilitating seamless data exchange among service providers [80].

8) Interoperability: Interoperability breaks significant barriers to seamless data exchange, often resulting in data silos where information is isolated and difficult to access across departments. The inefficiencies caused by these silos lead to redundant data collection efforts, increased operational costs, and delayed decision-making processes. Furthermore, the group of authors agreed that the absence of standardised data sharing frameworks exacerbates the complexity of managing and integrating data from multiple sources, making it challenging for the public sector to allow consistent and coherent public services [96], [105], [109], [117].

9) Governance: The authors [46] and [75] highlighted the role of blockchain in enhancing compliance, particularly in securing data access, protecting data privacy, and ensuring adherence to GDPR. Similarly, [67] demonstrates that blockchain-based e-archive systems improve the management of government information while maintaining compliance with the Public Sector Information (PSI) law. In contrast, [73] finds that the implementation of the European Timber Regulation (EUTR) remains complex, as it has not fully resolved longstanding challenges, thereby limiting traceability in the wood-energy sector. Furthermore, the introduction of new regulatory frameworks, such as the EU's Carbon Border Adjustment Mechanism (CBAM), has imposed additional responsibilities on government authorities to standardise compliance measures [52].

While blockchain technology holds significant promise for enhancing regulatory compliance, particularly in data management and privacy protection, it also comes with issues that need to be answered. The tension between blockchain's capabilities and existing legal frameworks, such as the GDPR [42], [61], highlights the need for ongoing dialogue and innovation to ensure that blockchain can be effectively integrated into regulatory environments. As new regulatory frameworks emerge, the role of blockchain in standardising compliance measures will continue to evolve, necessitating careful consideration of both technological and legal developments [79].

V. Discussion

A. Implications for E-Government Systems

Security concerns are a critical challenge in current data-sharing practices within e-government systems. With the increasing digitisation of government services, the volume of sensitive and personal data being shared across platforms has grown exponentially. This makes e-government systems prime targets for cyberattacks, data breaches, and unauthorised access. Traditional data-sharing methods often rely on centralised databases, which are vulnerable to hacking and can present a single point of failure. Once compromised, these databases can lead to the widespread leakage of sensitive information, undermining public trust in government services. Additionally, the lack of robust encryption and authentication mechanisms in many e-government systems leaves data vulnerable during transmission, further increasing the unauthorised access and interception risk.

Moreover, lack of transparency and accountability in current data-sharing practices limits public trust in e-government systems. Citizens often have little visibility into how their data is being used, shared, or stored by government agencies. This opacity can lead to concerns about data misuse, unauthorised sharing, or surveillance, which erodes confidence in digital government services. Additionally, when data-sharing processes are not transparent, the accuracy and integrity of the shared information are harder to verify, leading to potential errors or misinformation. This highlights the need for more transparent and accountable data-sharing mechanisms that can provide clear audit trails, ensure data integrity, and give citizens greater control and insight into how their data is handled.

In light of these challenges, there is a pressing need for more secure and efficient data-sharing solutions within e-government systems. Blockchain technology offers a promising avenue to address these limitations by offering a transparent, decentralised and secure platform for data sharing. By leveraging blockchain’s capabilities, e-government systems can overcome the challenges of data fragmentation, improve security, confirm fulfilment with privacy law, and improve public confidence in digital government services.

B. Theoretical Contributions

The result provides some tentative initial evidence to the literature on information security, blockchain security and e-government systems for data sharing. The study explored security factors involving blockchain in information security and e-government systems for data sharing. This has contributed to theoretical support in the field, supported by the findings.

Based on the systematic review conducted, nine theories of blockchain-based data sharing security factors are identified: confidentiality, integrity, availability, transparency, auditability, distributed, immutability, interoperability, and compliance have to answer RQ 3. With this brief description, the review also presents issues and solutions to various industries as an understanding of blockchain's ability to overcome constraints. Therefore, we show that blockchain technology is not limited to any industry that wants to implement cryptocurrency into its systems.

This new understanding should help to improve predictions of the impact of data sharing security factors that are involved in blockchain-based data sharing systems. Second, the study identifies the item under the factors in the literature that have a direct impact on securing data sharing. Thirdly, the conceptual framework has been developed as a reference in data sharing security using blockchain in e-government. Lastly, the research contributes to the body of knowledge on secure data sharing by investigating its use in the e-government domain.

Consequently, data sharing security factors and data security compliance are significant factors determining the causal effect of secure data sharing using blockchain technology. Previous research has shown that among way to assess the security of information systems is the development of a rating score using goal question metrics, which has specifically developed an instrument tool for cloud security [128], [129]. The author also presented how a security framework can be evaluated and applied in a real case scenario using the said approach.

C. Comparison with Existing Reviews

The landscape shows that blockchain has been widely accepted in improving the security of data sharing for the e-government system. The governance with legal requirements can be explored further towards the government data sharing policy for the e-government system. The research findings of [15] provide information on the adoption factors of blockchain based on the technology, organisation, and environment of the TOE methodology with added trust factors. With its key security factors of decentralisation, persistence, anonymity, and auditability, the author highlights how blockchain can transform security in conventional businesses. This research found that trust is the subfactor under confidentiality, while decentralize and auditability are the security factors in the findings. This research result also shows that persistency and anonymity are not in the security factors list in the literature for blockchain security.

Blockchain technology is also suitable to be applied across multiple e-government services. According to [130], blockchain is suitable for securing majority system purposes, including securing supply chains, managing records, amusement, and government. The five categories mentioned as confidential, trust, traceability, efficiency, and reliability are the features of blockchain applications proposed should also be categorized. This research uses various sources of information, including security reports and government policy, to give wider views of security factors in data sharing using blockchain, while the other authors only used journal articles for the review that which lack information from external sources and additional insights from industry information.

Blockchain technology offers promising opportunities for enhancing records and library operations, and its adoption is still in the nascent stages, where several challenges need to be addressed. Prior studies by [130] have noted the importance of blockchain challenges in libraries, which include technological barriers, financial constraints, legal and regulatory issues and social acceptance and awareness. Many scholars are of the view that the lack of empirical evidence and the need for highly qualified security personnel, financial resources, and regulatory compliance are significant barriers [23], [53], [69], [116], which supports the finding in this literature.

This study also discovered that the industry adopts blockchain because the technology behind it promises secure transactions, where the industry processes a huge amount of data to implement transparent storage through private transactions. This type of classification is expected to increase significantly, and it also remains a concern for various sectors in the long term because privacy and security are key aspects of establishing a decentralised transaction relationship with the industry. In contradiction of compliance factors, not all design principles were fully met, particularly regarding data access security and compliance with GDPR [74].

VI. Conclusion

This study found the invention taxonomy in blockchain research for the last 10 years. The most obvious finding that emerges from the analysis is that blockchain is a world-shattering technology that expressively transforms the way that e-government systems deliver a secure and trusted service. The significance of blockchain in the advancement and enhancement of data sharing security in e-government is provided. The recent analysis of the trend of security factors for data sharing was provided for the implementation of blockchain technology.

This review also shows the important discovery of secure data sharing using blockchain with various applications including securing supply chains, transportation, agriculture, healthcare and government administration. There are still opportunities for government agencies to apply or integrate blockchain technology to improve data security for their organisation. One unexpected finding was the extent to which trust and privacy the important factors in deploying the blockchain in e-government systems.

The most important finding is that data sharing security factors using blockchain can be classified into nine factors based on their application: confidentiality, integrity, availability, transparency, auditability, distributed, immutability, interoperability and governance. The most in-demand feature in blockchain applications is privacy enhancement, and the review of use cases presented.

These results have important implications for the development of blockchain as a platform to enhance data sharing security in government applications and innovations. The security factors involved in data sharing for e-government in the current research show that it persists with a significant impact in enhancing data security that is needed by the domain. This study focuses on the security factors for blockchain-based data sharing. The study did not cover the review for blockchain platform, architecture, consensus type and performance.

In the future, this study will lead to the development of a framework that covers the principles of data security, blockchain security and compliance. It also concludes that data sharing security could also significantly contribute towards the open data initiative. The understanding gained here should help to implement blockchain-based secured data sharing and increase trust in the e-government system.

REFERENCES

[1] I. Lykidis, G. Drosatos, and K. Rantos, “The use of blockchain technology in e-government services,” Dec. 01, 2021, MDPI. doi: 10.3390/computers10120168.

[2] L. T. Ha, “An investigation of digital integration’s importance on smart and sustainable agriculture in the European region,” Resources Policy, vol. 86, Oct. 2023, doi: 10.1016/j.resourpol.2023.104158.

[3] F. R. Batubara, J. Ubacht, and M. Janssen, “Challenges of blockchain technology adoption for e-government: a systematic literature review,” in Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age, in dg.o ’18. New York, NY, USA: Association for Computing Machinery, 2018. doi: 10.1145/3209281.3209317.

[4] Digital Department of Malaysia, “Fakta - Status pelaksanaan MyGDX sehingga kini,” 2025. Accessed: Jan. 28, 2025. [Online]. Available: https://www.mygdx.gov.my/ms/landing-page/facts?theme=second-theme

[5] MyCERT, “MyCERT _ Advisories - Cyber Incident Quarterly Summary Report - Q1 2025,” 2025, Accessed: Jul. 04, 2025. [Online]. Available: https://www.mycert.org.my/portal/advisory?id=SR-030.062025

[6] X. Zhang, T. Chen, Y. Feng, and Y. Yu, “A Data Sharing Scheme Based on Blockchain System and Attribute-Based Encryption,” in ACM International Conference Proceeding Series, Association for Computing Machinery, Mar. 2021, pp. 195–202. doi: 10.1145/3460537.3460559.

[7] S. F. Wamba, S. L. Wamba-Taguimdje, Q. Lu, and M. M. Queiroz, “How emerging technologies can solve critical issues in organizational operations: An analysis of blockchain-driven projects in the public sector,” Gov Inf Q, vol. 41, no. 1, Mar. 2024, doi: 10.1016/j.giq.2024.101912.

[8] B. Rukanova et al., “Realizing value from voluntary business-government information sharing through blockchain-enabled infrastructures: The case of importing tires to the Netherlands using TradeLens,” in ACM International Conference Proceeding Series, Association for Computing Machinery, Jun. 2021, pp. 505–514. doi: 10.1145/3463677.3463704.

[9] Information Commissioner’s Office - UK, “Data sharing: a code of practice,” 2021, Accessed: Dec. 24, 2024. [Online]. Available: https://ico.org.uk/media2/ictfahk2/data-sharing-a-code-of-practice-all-1-0-2.pdf

[10] M. Nieles, K. Dempsey, and V. Y. Pillitteri, “An introduction to information security,” Gaithersburg, MD, Jun. 2017. doi: 10.6028/NIST.SP.800-12r1.

[11] National Institute of Standards and Technology, “The NIST Cybersecurity Framework (CSF) 2.0,” Feb. 2024. doi: 10.6028/NIST.CSWP.29.

[12] U.S. Government Publishing Office, “Chapter 35 - Coordination of Federal Information Policy Subchapter III - Information Security,” Dec. 2002, Accessed: Oct. 01, 2025. [Online]. Available: https://www.govinfo.gov/content/pkg/USCODE-2011-title44/html/USCODE-2011-title44-chap35-subchapIII-sec3542.htm

[13] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” Decentralized business review, p. 21260, 2008. [Online]. Available: www.bitcoin.org

[14] O. Konashevych, “‘GoLand Registry’ Case Study,” in ACM International Conference Proceeding Series, Association for Computing Machinery, Jun. 2021, pp. 489–494. doi: 10.1145/3463677.3463720.

[15] M. S. Kamarulzaman, N. H. Hassan, N. A. A. Bakar, N. Maarop, G. A. L. N. Samy, and N. Aziz, “Factors Influencing Blockchain Adoption in Government Organization : A Proposed Framework,” in Proceedings - International Conference on Computer and Information Sciences: Sustaining Tomorrow with Digital Innovation, ICCOINS 2021, Institute of Electrical and Electronics Engineers Inc., Jul. 2021, pp. 366–371. doi: 10.1109/ICCOINS49721.2021.9497196.

[16] J. Guo, Y. Bai, S. Sun, F. Liu, and J. Yang, “E-government System Based on Blockchain,” in 2023 3rd International Conference on Digital Society and Intelligent Systems, DSInS 2023, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 449–452. doi: 10.1109/DSInS60115.2023.10455503.

[17] Unit Permodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU), Dasar Perkongsian Data Sektor Awam. 2021. Accessed: Sep. 06, 2023. [Online]. Available: https://dasar.mampu.gov.my/search-g/download-file/258/e8542746051d6cfbc33a61bd16be0ee7

[18] Parliament of Malaysia, Act 864 - DATA SHARING ACT 2025. 2025. Accessed: Mar. 04, 2025. [Online]. Available: https://lom.agc.gov.my/ilims/upload/portal/akta/outputaktap/2687068_BI/Act%20864%20-%20DATA%20SHARING%20ACT%202025.pdf

[19] M. J. Page et al., “The PRISMA 2020 statement: An updated guideline for reporting systematic reviews,” Mar. 29, 2021, BMJ Publishing Group. doi: 10.1136/bmj.n71.

[20] V. Buterin, “Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform.,” 2014. Accessed: Feb. 23, 2025. [Online]. Available: https://ethereum.org/content/whitepaper/whitepaper-pdf/Ethereum_Whitepaper_-_Buterin_2014.pdf

[21] Chong Shen, Kun Zhang, and Keliu Long, “Research on Hainan Trusted Digital Infrastructure Construction Framework,” in 29th Wireless and Optical Communications Conference (WOCC), IEEE, 2020.

[22] L. Cai and S. Yao, “Application of big data technology in blockchain computing,” in 2nd International Conference on Artificial Intelligence and Information Systems (ICAIIS ’21), ACM, 2021. doi: 10.1145/3469213.

[23] D. Zhang, L. G. Pee, S. L. Pan, and L. Cui, “Big data analytics, resource orchestration, and digital sustainability: A case study of smart city development,” Gov Inf Q, vol. 39, no. 1, Jan. 2022, doi: 10.1016/j.giq.2021.101626.

[24] H. Hou, “The application of blockchain technology in E-government in China,” in 26th International Conference on Computer Communication and Networks (ICCCN), IEEE, 2017.

[25] J. Bao, X. Geng, and P. Yu, “An digital economy mode based on blockchain,” in Proceedings - 2020 International Conference on Robots and Intelligent Systems, ICRIS 2020, Institute of Electrical and Electronics Engineers Inc., Nov. 2020, pp. 391–394. doi: 10.1109/ICRIS52159.2020.00102.

[26] G. Huang, D. Li, S. T. Ng, L. Wang, and T. Wang, “A methodology for assessing supply-demand matching of smart government services from citizens’ perspective: A case study in Nanjing, China,” Habitat Int, vol. 138, Aug. 2023, doi: 10.1016/j.habitatint.2023.102880.

[27] L. Liu, C. Piao, X. Jiang, and L. Zheng, “Research on Governmental Data Sharing Based on Local Differential Privacy Approach,” in Proceedings - 2018 IEEE 15th International Conference on e-Business Engineering, ICEBE 2018, Institute of Electrical and Electronics Engineers Inc., Dec. 2018, pp. 39–45. doi: 10.1109/ICEBE.2018.00017.

[28] Y. Zhang, S. Deng, Y. Zhang, and J. Kong, “Research on government information sharing model using blockchain technology,” in Proceedings - 10th International Conference on Information Technology in Medicine and Education, ITME 2019, Institute of Electrical and Electronics Engineers Inc., Aug. 2019, pp. 726–729. doi: 10.1109/ITME.2019.00166.

[29] C. Xu, H. Yang, Q. Yu, and Z. Li, “Trusted and Flexible Electronic Certificate Catalog Sharing System Based on Consortium Blockchain,” in

IEEE 5th International Conference on Computer and Communications (ICCC), IEEE, 2019.

[30] M. Sun and J. Zhang, “Research on the application of block chain big data platform in the construction of new smart city for low carbon emission and green environment,” Comput Commun, vol. 149, pp. 332–342, Jan. 2020, doi: 10.1016/j.comcom.2019.10.031.

[31] H. Zhang and W. Liu, “Research on the Application of Blockchain in the Safe and Trusted Sharing of Government Data,” in Proceedings - 2023 2nd International Conference on Artificial Intelligence and Blockchain Technology, AIBT 2023, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 52–55. doi: 10.1109/AIBT57480.2023.00017.

[32] A. U. Khan, Z. Zhang, M. Taleby Ahvanooey, and W. Rafique, “Opinion mining towards blockchain technology adoption for accessing digital library resources,” Aslib Journal of Information Management, vol. 74, no. 1, pp. 135–157, Jan. 2022, doi: 10.1108/AJIM-01-2021-0016.

[33] S. S. Kamble, A. Gunasekaran, and R. Sharma, “Modeling the blockchain enabled traceability in agriculture supply chain,” Int J Inf Manage, vol. 52, Jun. 2020, doi: 10.1016/j.ijinfomgt.2019.05.023.

[34] A. Patil, V. Shardeo, A. Dwivedi, and J. Madaan, “An integrated approach to model the blockchain implementation barriers in humanitarian supply chain,” Journal of Global Operations and Strategic Sourcing, vol. 14, no. 1, pp. 81–103, Mar. 2021, doi: 10.1108/JGOSS-07-2020-0042.

[35] A. Kumar, “Improvement of public distribution system efficiency applying blockchain technology during pandemic outbreak (COVID-19),” Journal of Humanitarian Logistics and Supply Chain Management, vol. 11, no. 1, pp. 1–28, Feb. 2021, doi: 10.1108/JHLSCM-06-2020-0050.

[36] S. Bakare, S. C. Shinde, and R. Hubballi, “A Blockchain Framework for secure Digital Identity transactions in Indian Agri-subsidy system: Issues, challenges and benefits,” in Proceedings of the 2021 4th International Conference on Computing and Communications Technologies, ICCCT 2021, Institute of Electrical and Electronics Engineers Inc., 2021, pp. 138–143. doi: 10.1109/ICCCT53315.2021.9711868.

[37] A. Jain, D. Desai, and R. Sangole, “A Case Study on Use of Blockchain Technology as a Dominant Feature to Issue and Verify Documents Required for Admission to UG/PG Technical Programs in Maharashtra (India),” in 2022 IEEE Pune Section International Conference, PuneCon 2022, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/PuneCon55413.2022.10014917.

[38] S. Panchamia and D. K. Byrappa, “Passport, VISA and Immigration Management Using Blockchain,” in Proceedings - 23rd Annual Conference on Advanced Computing and Communications, ADCOM 2017, Institute of Electrical and Electronics Engineers Inc., Jul. 2017, pp. 8–17. doi: 10.1109/ADCOM.2017.00009.

[39] N. P. Rana, Y. K. Dwivedi, and D. L. Hughes, “Analysis of challenges for blockchain adoption within the Indian public sector: an interpretive structural modelling approach,” Information Technology and People, vol. 35, no. 2, pp. 548–576, Mar. 2022, doi: 10.1108/ITP-07-2020-0460.

[40] M. Bakhtina, R. Matulevičius, A. Awad, and P. Kivimäki, “On the Shift to Decentralised Identity Management in Distributed Data Exchange Systems,” in Proceedings of the ACM Symposium on Applied Computing, Association for Computing Machinery, Mar. 2023, pp. 864–873. doi: 10.1145/3555776.3577678.

[41] S. Bali, V. Bali, R. P. Mohanty, and D. Gaur, “Analysis of critical success factors for blockchain technology implementation in healthcare sector,” Benchmarking, vol. 30, no. 4, pp. 1367–1399, Apr. 2023, doi: 10.1108/BIJ-07-2021-0433.

[42] S. Ølnes and Arild. Janssen, “Blockchain Technology as Infrastructure in Public Sector – an Analytical Framework,” in Norwegian Conference on ICT in the public sector (NOKIOS), ACM, 2018.

[43] S. N. Khan, M. Shael, and M. Majdalawieh, “Blockchain technology as a support infrastructure in E-Government evolution at Dubai economic department,” in ACM International Conference Proceeding Series, Association for Computing Machinery, Jul. 2019, pp. 124–130. doi: 10.1145/3343147.3343164.

[44] A. Farouk, A. Alahmadi, S. Ghose, and A. Mashatan, “Blockchain platform for industrial healthcare: Vision and future opportunities,” Mar. 15, 2020, Elsevier B.V. doi: 10.1016/j.comcom.2020.02.058.

[45] H. Scholta, W. Mertens, M. Kowalkiewicz, and J. Becker, “From one-stop shop to no-stop shop: An e-government stage model,” Gov Inf Q, vol. 36, no. 1, pp. 11–26, Jan. 2019, doi: 10.1016/j.giq.2018.11.010.

[46] A. Alahbabi, K. Alshehhi, A. Albloushi, and K. Shuaib, “Establishing Security Controls For Blockchain Technology In P2P Energy Trading,” in 2023 IEEE PES Conference on Innovative Smart Grid Technologies - Middle East, ISGT Middle East 2023 - Proceedings, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/ISGTMiddleEast56437.2023.10078508.

[47] O. Hujran, M. M. Al-Debei, A. S. Al-Adwan, A. Alarabiat, and N. Altarawneh, “Examining the antecedents and outcomes of smart government usage: An integrated model,” Gov Inf Q, vol. 40, no. 1, Jan. 2023, doi: 10.1016/j.giq.2022.101783.

[48] G. Spiga, S. Z. Ahmad, and W. Yeoh, “Blockchain adoption impact on real estate performance: the mediating role of real estate and blockchain transparency,” Business Process Management Journal, 2024, doi: 10.1108/BPMJ-09-2023-0701.

[49] M. F. Körner, J. Sedlmeir, M. Weibelzahl, G. Fridgen, M. Heine, and C. Neumann, “Systemic risks in electricity systems: A perspective on the potential of digital technologies,” Energy Policy, vol. 164, May 2022, doi: 10.1016/j.enpol.2022.112901.

[50] L. Klug and W. Prinz, “Fair prices for sustainability in agriculture and food. Requirements and design options for a data-based transparency system.,” in ACM International Conference Proceeding Series, Association for Computing Machinery, Jul. 2023, pp. 496–507. doi: 10.1145/3598469.3598525.

[51] B. Rukanova et al., “A Framework for Understanding Circular Economy Monitoring: Insights from the Automotive Industry,” in ACM International Conference Proceeding Series, Association for Computing Machinery, Jul. 2023, pp. 544–555. doi: 10.1145/3598469.3598530.

[52] B. Rukanova et al., “Public value creation through voluntary business to government information sharing enabled by digital infrastructure innovations: a framework for analysis,” Gov Inf Q, vol. 40, no. 2, Apr. 2023, doi: 10.1016/j.giq.2022.101786.

[53] M. Brinkmann and M. Heine, “The Implementation of New Public Governance Through Blockchain: A Delphi-based analysis,” in ACM International Conference Proceeding Series, Association for Computing Machinery, Oct. 2022, pp. 1–9. doi: 10.1145/3560107.3560108.

[54] L. M. Baltruschat, V. Jaiman, and V. Urovi, “User acceptability of blockchain technology for enabling electronic health record exchange,” Journal of Systems and Information Technology, vol. 25, no. 3, pp. 268–295, 2023, doi: 10.1108/JSIT-09-2022-0225.

[55] I. Azogu, A. Norta, I. Papper, J. Longo, and D. Draheim, “A framework for the adoption of blockchain technology in healthcare information management systems: A case study of Nigeria,” in ACM International Conference Proceeding Series, Association for Computing Machinery, 2019, pp. 310–316. doi: 10.1145/3326365.3326405.

[56] D. W. Bates, A. Heitmueller, M. Kakad, and S. Saria, “Why policymakers should care about ‘big data’ in healthcare,” Health Policy Technol, vol. 7, no. 2, pp. 211–216, Jun. 2018, doi: 10.1016/j.hlpt.2018.04.006.

[57] G. Tshering and S. Gao, “Understanding security in the government’s use of blockchain technology with value focused thinking approach,” Journal of Enterprise Information Management, vol. 33, no. 3, pp. 519–540, Apr. 2020, doi: 10.1108/JEIM-06-2018-0138.

[58] T. Ly. Charles and A. A. Azeta, “A Blockchain Framework for Securing Examination Results in Higher Institutions of Learning,” in International Conference on Science, Engineering and Business for Driving Sustainable Development Goals, SEB4SDG 2024, Institute of Electrical and Electronics Engineers Inc., 2024. doi: 10.1109/SEB4SDG60871.2024.10630246.

[59] A. Ahmad, M. Saad, M. Bassiouni, and A. Mohaisen, “Towards Blockchain-Driven, Secure and Transparent Audit Logs,” in Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, in MobiQuitous ’18. New York, NY, USA: Association for Computing Machinery, 2018, pp. 443–448. doi: 10.1145/3286978.3286985.

[60] C. M. Adilieme, R. B. Abidoye, and C. L. Lee, “Barriers and prospects for the adoption of blockchain technology in property valuation,” Journal

of European Real Estate Research, 2024, doi: 10.1108/JERER-04-2024-0022.

[61] A. Shahaab, I. A. Khan, R. Maude, C. Hewage, and Y. Wang, "Public service operational efficiency and blockchain – A case study of Companies House, UK," Gov Inf Q, vol. 40, no. 1, Jan. 2023, doi: 10.1016/j.giq.2022.101759.

[62] M. A. Sicilia and A. Visvizi, "Blockchain and OECD data repositories: opportunities and policymaking implications," Library Hi Tech, vol. 37, no. 1, pp. 30–42, Mar. 2019, doi: 10.1108/LHT-12-2017-0276.

[63] E. A. Akartuna, S. D. Johnson, and A. Thornton, "Preventing the money laundering and terrorist financing risks of emerging technologies: An international policy Delphi study," Technol Forecast Soc Change, vol. 179, Jun. 2022, doi: 10.1016/j.techfore.2022.121632.

[64] A. Azmi, F. Yahya, E. G. Moung, H. Sallehudin, R. G. Utomo, and N. A. Azman, "Blockchain-based Data Sharing Framework for Malaysia Government Aid Management System," in 2023 International Conference on Digital Applications, Transformation and Economy, ICDATE 2023, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/ICDATE58146.2023.10248471.

[65] K. Biswas and V. Muthukkumarasamy, "Securing Smart Cities Using Blockchain Technology," 2016, doi: 10.1109/HPCC-SmartCity-DSS.2016.178.

[66] E. Acosta Llano, P. Hurmelinna-Laukkanen, and L. Haapanen, "Blockchain for the circular economy, implications for public governance," International Journal of Public Sector Management, 2024, doi: 10.1108/IJPSM-12-2023-0365.

[67] P. Svärd and E. Borglund, "The implementation of an e-archive to facilitate open data publication and the use of common specifications: A case of three Swedish agencies," Gov Inf Q, vol. 39, no. 4, Oct. 2022, doi: 10.1016/j.giq.2022.101751.

[68] H. J. Rim, "Decentralized identity (DID): new technology adoption and diffusion in South Korea," Transforming Government: People, Process and Policy, vol. 17, no. 2, pp. 251–270, Apr. 2023, doi: 10.1108/TG-11-2021-0189.

[69] D. S. K. Putra and A. Alfari, "IDNat-Blockchain: A Concept for Indonesia's National Blockchain," in Proceeding - 2021 2nd International Conference on ICT for Rural Development, IC-ICTRuDev 2021, Institute of Electrical and Electronics Engineers Inc., 2021. doi: 10.1109/IC-ICTRuDev50538.2021.9656496.

[70] A. Ghaffar and M. Hussain, "BCEAP – A blockchain embedded academic paradigm to augment legacy education through application," in ACM International Conference Proceeding Series, Association for Computing Machinery, Jul. 2019. doi: 10.1145/3341325.3342036.

[71] P. Baudier, G. Kondrateva, C. Ammi, and E. Seulliet, "Peace engineering: The contribution of blockchain systems to the e-voting process," Technol Forecast Soc Change, vol. 162, Jan. 2021, doi: 10.1016/j.techfore.2020.120397.

[72] T. Nodehi, A. Zutshi, A. Grilo, and B. Rizvanovic, "EBDF: The enterprise blockchain design framework and its application to an e-Procurement ecosystem," Comput Ind Eng, vol. 171, Sep. 2022, doi: 10.1016/j.cie.2022.108360.

[73] S. Ciliberti et al., "EUTR implementation in the Italian wood-energy sector: Role and impact of (ongoing) digitalisation," Aug. 01, 2022, Elsevier B.V. doi: 10.1016/j.forpol.2022.102758.

[74] J. S. Søgaard, "A blockchain-enabled platform for VAT settlement," International Journal of Accounting Information Systems, vol. 40, Mar. 2021, doi: 10.1016/j.accinf.2021.100502.

[75] F. E. Tanha, A. Hasani, S. Hakak, and T. R. Gadekallu, "Blockchain-based cyber physical systems: Comprehensive model for challenge assessment," Computers and Electrical Engineering, vol. 103, Oct. 2022, doi: 10.1016/j.compeleceng.2022.108347.

[76] A. Alkhaldi, H. Alrashidi, K. Alhasan, A. Alsadeeqi, and A. Alshami, "The use of blockchain technology to build smart cities: creating public value in Kuwait," Global Knowledge, Memory and Communication, 2023, doi: 10.1108/GKMC-11-2022-0263.

[77] A. H. Dbesan, A. A. Abdulmuhsin, and A. F. Alkhwaldi, "Adopting knowledge-sharing-driven blockchain technology in healthcare: a developing country's perspective," VINE Journal of Information and Knowledge Management Systems, 2023, doi: 10.1108/VJIKMS-01-2023-0021.

[78] L. Cai and S. Yao, "Application of big data technology in blockchain computing," in 2021 2nd International Conference on Artificial Intelligence and Information Systems, in ICAIIS 2021. New York, NY, USA: Association for Computing Machinery, 2021. doi: 10.1145/3469213.3470409.

[79] T. Chen, Y. Yu, Z. Duan, J. Gao, and K. Lan, "BlockChain/ABE-based Fusion Solution for E-government Data Sharing and Privacy protection," in ACM International Conference Proceeding Series, Association for Computing Machinery, Nov. 2020, pp. 258–264. doi: 10.1145/3443467.3443764.

[80] S. T. Jagtap, C. M. Thakar, O. El Imrani, K. Phasinam, S. Garg, and R. J. M. Ventayen, "A Framework for Secure Healthcare System Using Blockchain and Smart Contracts," in Proceedings of the 2nd International Conference on Electronics and Sustainable Communication Systems, ICESC 2021, Institute of Electrical and Electronics Engineers Inc., Aug. 2021, pp. 922–926. doi: 10.1109/ICESC51422.2021.9532644.

[81] K. Kumutha and S. Jayalakshmi, "Hyperledger Fabric Blockchain Framework: Efficient Solution for Academic Certificate Decentralized Repository," in Proceedings of the 5th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), I-SMAC 2021, Institute of Electrical and Electronics Engineers Inc., 2021, pp. 1584–1590. doi: 10.1109/I-SMAC52330.2021.9640785.

[82] S. Singh, S. Rathore, O. Alfarraj, A. Tolba, and B. Yoon, "A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology," Future Generation Computer Systems, vol. 129, pp. 380–388, Apr. 2022, doi: 10.1016/j.future.2021.11.028.

[83] Y. Li, M. K. Lim, and C. Wang, "An intelligent model of green urban distribution in the blockchain environment," Resour Conserv Recycl, vol. 176, Jan. 2022, doi: 10.1016/j.resconrec.2021.105925.

[84] S. Saxena, D. Shao, A. Nikiforova, and R. Thapliyal, "Invoking blockchain technology in e-government services: a cybernetic perspective," Digital Policy, Regulation and Governance , vol. 24, no. 3, pp. 246–258, Jun. 2022, doi: 10.1108/DPRG-10-2021-0128.

[85] J. Xu, C. Hua, and Y. Zhang, "A Blockchain-Based Framework for Supervision of Livelihood Issues: Proof of Concept With Optimized Consensus," IEEE Access, vol. 11, pp. 73414–73434, 2023, doi: 10.1109/ACCESS.2023.3295696.

[86] K. Shruthi and A. S. Poornima, "A Transparent and Privacy-Preserving Job Search Platform Built on the Ethereum Blockchain Framework," in Proceedings of 2023 IEEE 2nd International Conference on Industrial Electronics: Developments and Applications, ICIDeA 2023, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 235–242. doi: 10.1109/ICIDeA59866.2023.10295065.

[87] P. Rede, S. Iyer, S. Sharma, and S. Deshmukh, "Blockchain Based Identity Management System Using Cryptography and Steganography," in 2023 International Conference on Information Technology: Cybersecurity Challenges for Sustainable Cities, ICIT 2023 - Proceeding, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 173–177. doi: 10.1109/ICIT58056.2023.10225957.

[88] S. Peng, D. Sun, L. Zhu, H. Zhou, X. Zhang, and C. Cui, "Enhancing Cross-Border Data Sharing in Blockchain Networks: A Compliance-Centric Approach Ensuring Anonymity and Traceability," in 2023 3rd International Conference on Computer Science and Blockchain, CCSB 2023, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 200–204. doi: 10.1109/CCSB60789.2023.10398873.

[89] J. Du, Z. Xu, D. Liu, X. Zhang, and H. Cheng, "EPT: Enhancing User Transparency for Confidential Smart Contract," in Proceedings - 2023 19th International Conference on Mobility, Sensing and Networking, MSN 2023, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 431–438. doi: 10.1109/MSN60784.2023.00069.

[90] S. Siddiqui, S. Hameed, S. A. Shah, A. K. Khan, and A. Aneiba, "Smart contract-based security architecture for collaborative services in municipal smart cities[Formula presented]," Journal of Systems Architecture, vol. 135, Feb. 2023, doi: 10.1016/j.sysarc.2022.102802.

[91] S. Capraz and A. Ozsoy, "A Secure Medical Data Sharing Framework for Fight Against Pandemics Like Covid-19 by Using Public Blockchain," IEEE Access, vol. 12, pp. 93593–93605, 2024, doi: 10.1109/ACCESS.2024.3423714.

[92] R. Raj, A. Singh, V. Kumar, and P. Verma, “Challenges in adopting blockchain technology in supply chain management: a too far fetched idea?,” International Journal of Quality and Reliability Management, vol. 41, no. 8, pp. 2146–2180, Sep. 2024, doi: 10.1108/IJQRM-12-2022-0366.

[93] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, “On blockchain and its integration with IoT. Challenges and opportunities,” Future Generation Computer Systems, vol. 88, pp. 173–190, Nov. 2018, doi: 10.1016/j.future.2018.05.046.

[94] Deepayan Bhowmik, Ambarish Natu, Takaaki Ishikawa, Tian Feng, and Charith Abhayaratne, “THE JPEG-BLOCKCHAIN FRAMEWORK FOR GLAM SERVICES,” in IEEE International Conference on Multimedia and Expo (ICME), IEEE, 2018.

[95] W. Fan, H. J. Hong, X. Zhou, and S. Y. Chang, “A Generic Blockchain Framework to Secure Decentralized Applications,” in IEEE International Conference on Communications, Institute of Electrical and Electronics Engineers Inc., Jun. 2021. doi: 10.1109/ICC42927.2021.9500924.

[96] D. Sinha and S. Roy Chowdhury, “Blockchain-based smart contract for international business – a framework,” Journal of Global Operations and Strategic Sourcing, vol. 14, no. 1, pp. 224–260, Mar. 2021, doi: 10.1108/JGOSS-06-2020-0031.

[97] C. Piao, Y. Hao, J. Yan, and X. Jiang, “Privacy preserving in blockchain-based government data sharing: A Service-On-Chain (SOC) approach,” Inf Process Manag, vol. 58, no. 5, Sep. 2021, doi: 10.1016/j.ipm.2021.102651.

[98] F. H. L. Chong, “Enhancing trust through digital Islamic finance and blockchain technology,” Qualitative Research in Financial Markets, vol. 13, no. 3, pp. 328–341, 2021, doi: 10.1108/QRFM-05-2020-0076.

[99] M. Elbialy, M. A. Elsalam, and S. A. El-Fotouh, “A Framework for Enhancing the Supply of Scientific Research Projects Using Blockchain,” in 5th International Conference on Computing and Informatics, ICCI 2022, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 140–147. doi: 10.1109/ICCI54321.2022.9756099.

[100]J. Wang, H. Jin, J. Chen, J. Tan, and K. Zhong, “Anomaly detection in Internet of medical Things with Blockchain from the perspective of deep neural network,” Inf Sci (N Y), vol. 617, pp. 133–149, Dec. 2022, doi: 10.1016/j.ins.2022.10.060.

[101]C. Turhan and I. Akman, “Exploring sectoral diversity in the timing of organizational blockchain adoption,” Information Technology and People, vol. 35, no. 7, pp. 1912–1930, Dec. 2022, doi: 10.1108/ITP-05-2020-0330.

[102]K. Saurabh, P. Upadhyay, and N. Rani, “A study on blockchain-based marketplace governance platform adoption: a multi-industry perspective,” Nov. 09, 2023, Emerald Publishing. doi: 10.1108/DPRG-04-2023-0053.

[103]W. Shang and Z. Yu, “A new media content trusted dissemination architecture based on AV-blockchain and ChinaDRM,” Intelligent and Converged Networks, vol. 4, no. 2, pp. 142–157, Jun. 2023, doi: 10.23919/ICN.2023.0015.

[104]V. Malik et al., “Building a Secure Platform for Digital Governance Interoperability and Data Exchange Using Blockchain and Deep Learning-Based Frameworks,” IEEE Access, vol. 11, pp. 70110–70131, 2023, doi: 10.1109/ACCESS.2023.3293529.

[105]C. B. Basha et al., “Fostering Effective Cyber Threat Intelligence Sharing: Overcoming Challenges and Implementing Best Practices,” in International Conference for Technological Engineering and its Applications in Sustainable Development, ICTEASD 2023, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 177–182. doi: 10.1109/ICTEASD57136.2023.10585133.

[106]M. Naudiyal et al., “Secure Blockchain-based Framework for Smart City Applications,” in 2023 World Conference on Communication and Computing, WCONF 2023, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/WCONF58270.2023.10235249.

[107]Y. Tian, B. Liu, Y. Li, P. Szalachowski, and J. Zhou, “Accountable Fine-Grained Blockchain Rewriting in the Permissionless Setting,” IEEE Transactions on Information Forensics and Security, vol. 19, pp. 1756–1766, 2024, doi: 10.1109/TIFS.2023.3340917.

[108]T. Nhan, K. Upadhyay, and K. Poudel, “Towards Patient-Centric Healthcare: Leveraging Blockchain for Electronic Health Records,” in SIGMIS-CPR 2024 - Proceedings of the Computers and People Research Conference: Trust and Legitimacy in Emerging Technologies: Organizational and Societal Implications for People, Places and Power, Association for Computing Machinery, Inc, May 2024. doi: 10.1145/3632634.3655883.

[109]L. Zavolokina, I. Bauer-Hänsel, J. Hacker, and G. Schwabe, “Organizing for value creation in blockchain information systems,” Information and Organization, vol. 34, no. 3, Sep. 2024, doi: 10.1016/j.infoandorg.2024.100522.

[110]N. Goderdzishvili, E. Gordadze, and N. Gagnidze, “Georgia’s blockchain-powered property registration: Never blocked, always secured - Ownership data kept best!,” in ACM International Conference Proceeding Series, Association for Computing Machinery, Apr. 2018, pp. 673–675. doi: 10.1145/3209415.3209437.

[111]O. Konashevych, “Cross-blockchain protocol for public registries,” International Journal of Web Information Systems, vol. 16, no. 5, pp. 571–610, Nov. 2020, doi: 10.1108/IJWIS-07-2020-0045.

[112]Y. Liu and J. Zeng, “Government Data Sharing based on Blockchain,” in ACM International Conference Proceeding Series, Association for Computing Machinery, Mar. 2021, pp. 123–128. doi: 10.1145/3460537.3460562.

[113]S. Yu, T. Zhang, X. Huang, and X. Xia, “Design and Implementation of a Blockchain-Based Road Damage Approval System,” in ACM International Conference Proceeding Series, Association for Computing Machinery, May 2022, pp. 94–103. doi: 10.1145/3538950.3538963.

[114]Z. Pan, D. Wu, and M. Liu, “Evaluation Study on the Level of Ecological Governance of Digital Intelligence in Beijing,” in ACM International Conference Proceeding Series, Association for Computing Machinery, Sep. 2023, pp. 327–333. doi: 10.1145/3629378.3629400.

[115]Y. Du, J. Yuan, S. Q. Wang, Y. Liu, and N. Zeng, “Leveraging blockchain to anchor information for supervision in PPP projects: a conceptual framework,” Engineering, Construction and Architectural Management, 2024, doi: 10.1108/ECAM-07-2023-0758.

[116]G. P. Andrade, J. C. A. de Abreu, and R. C. dos Santos, “The impact of blockchain on Brazilian public procurement processes from the perspective of transaction costs: scenarios as perceived by experts,” International Journal of Organizational Analysis, 2024, doi: 10.1108/IJOA-07-2023-3829.

[117]N. Lalchandani, F. Jiang, J. J. Jeong, Y. Zolotavkin, and R. Doss, “Evaluating the Current State of Application Programming Interfaces for Verifiable Credentials,” in 2021 18th International Conference on Privacy, Security and Trust, PST 2021, Institute of Electrical and Electronics Engineers Inc., 2021. doi: 10.1109/PST52912.2021.9647805.

[118]S. Luthra, M. Janssen, N. P. Rana, G. Yadav, and Y. K. Dwivedi, “Categorizing and relating implementation challenges for realizing blockchain applications in government,” Information Technology and People, vol. 36, no. 4, pp. 1580–1602, May 2023, doi: 10.1108/ITP-08-2020-0600.

[119]A. Aytekin et al., “A bipolar neutrosophic combined compromise solution-based hybrid model for identifying blockchain application barriers and Benchmarking consensus algorithms,” Eng Appl Artif Intell, vol. 133, Jul. 2024, doi: 10.1016/j.engappai.2024.108343.

[120]M. J. M. Chowdhury, A. Colman, M. A. Kabir, J. Han, and P. Sarda, “Blockchain as a Notarization Service for Data Sharing with Personal Data Store,” in Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018, Institute of Electrical and Electronics Engineers Inc., Sep. 2018, pp. 1330–1335. doi: 10.1109/TrustCom/BigDataSE.2018.00183.

[121]Veselin Monev, “Measuring the Optimal Information Security Complexity for Blockchain Operations,” in IEEE International Conference on Information Technologies (InfoTech-2020), IEEE, 2020.

[122]Y. Lin et al., “Power Data Blockchain Sharing Scheme based on Homomorphic Encryption,” in IMCEC 2022 - IEEE 5th Advanced Information Management, Communicates, Electronic and Automation Control Conference, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 625–629. doi: 10.1109/IMCEC55388.2022.10020058.

[123]X. Yao, X. Cheng, Z. Shi, K. Liu, M. Liu, and Y. Li, “Using Blockchain to Share Data Securely in the IntelliSense Environment,” in Proceedings

- 2022 International Conference on Blockchain Technology and Information Security, ICBCTIS 2022, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 106–110. doi: 10.1109/ICBCTIS55569.2022.00035.

[124] W. Yang, Z. Guan, L. Wu, X. Du, and M. Guizani, “Secure Data Access Control with Fair Accountability in Smart Grid Data Sharing: An Edge Blockchain Approach,” IEEE Internet Things J, vol. 8, no. 10, pp. 8632–8643, May 2021, doi: 10.1109/JIOT.2020.3047640.

[125] S. Ølnes, J. Ubacht, and M. Janssen, “Blockchain in government: Benefits and implications of distributed ledger technology for information sharing,” Sep. 01, 2017, Elsevier Ltd. doi: 10.1016/j.giq.2017.09.007.

[126] D. B. Rawat and A. Alshaikhi, “Leveraging Distributed Blockchain-based Scheme for Wireless Network Virtualization with Security and QoS Constraints,” 2018.

[127] G. Subramanian and A. S. Thampy, “Blockchain Consortium for Electric Vehicles to Enhance the Security,” in 2022 International Conference for Advancement in Technology, ICONAT 2022, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/ICONAT53423.2022.9725887.

[128] F. Yahya, R. J. Walters, and G. B. Wills, “Goal-based security components for cloud storage security framework: A preliminary study,” in 2016 International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2016, Institute of Electrical and Electronics Engineers Inc., Jun. 2016. doi: 10.1109/CyberSecPODS.2016.7502338.

[129] F. Yahya, R. J. Walters, and G. B. Wills, “Using Goal-Question-Metric (GQM) approach to assess security in cloud storage,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Springer Verlag, 2017, pp. 223–240. doi: 10.1007/978-3-319-54380-2_10.

[130] D. Benz, M. Hamzah, M. F. Ghazali, and M. F. Asli, “Bringing Blockchain Technology in Innovating Industries: A Systematic Review,” in Lecture Notes in Networks and Systems, Springer Science and Business Media Deutschland GmbH, 2022, pp. 391–416. doi: 10.1007/978-3-030-85990-9_33.