NOVA IMS Information Management School

MGI

Master's Degree Program in

Information Management

"Consortium Blockchain in E-Government & Smart Democracy"

Learning from the past for the future:
How the data more effective and secure in the context of consortium blockchain

Shaheen Aamir

Dissertation

presented as a partial requirement for obtaining the Master Degree Program in Information Management

NOVA Information Management School

Instituto Superior de Estatística e Gestão de Informação

Universidade Nova de Lisboa

NOVA Information Management School

Instituto Superior de Estatística e Gestão de Informação

Universidade Nova de Lisboa

"Consortium Blockchain in E-Government and Smart Democracy"

By

Shaheen Aamir

Dissertation presented as a partial requirement for obtaining the Master's degree in Information Management, with a specialization in Information System and Technologies

Supervisor: Vitor Manuel Pereira Duarte dos Santos

November 2023

STATEMENT OF INTEGRITY

I thus certify that I carried out my academic work in an ethical manner. I certify that while developing this work, I did not employ any plagiarism, excessive use of information, or falsification of results. I also hereby affirm that I have read and understood the NOVA Information Management School's Code of Honor and Rules of Conduct.

Shaheen Aamir

[Lisbon, Nov 2023]

ACKNOWLEDGEMENT

I am profoundly grateful to Professor Vitor Duarte who has provided me with consistent mentorship and advice throughout my thesis journey, for which I am incredibly thankful. The quality and depth of my work have been greatly influenced by his priceless insights and unwavering support. I want to express my sincere gratitude to the Nova IMS Institute for offering invaluable materials that have greatly enhanced the study process. This thesis's accomplishment was largely made possible by having access to these resources. I also want to sincerely thank my husband, Aamir Nadeem, for his unwavering encouragement, understanding, and support during this academic journey. The feat would not have been feasible without the combined efforts of these extraordinary people and organizations, which are honored in this thesis.

ABSTRACT

The public administration field is undergoing a revolution due to the rise of digital technologies. Prior to the digital revolution, public management was frequently marked by bureaucratic obstacles, low democratic involvement, and inefficiency. This thesis investigates how blockchain technology might change existing procedures, promoting citizen confidence, government accountability, and openness. A design science research strategy was used to do this, utilizing systematic literature reviews to learn about the most recent findings on blockchain technology in the context of e-governance and referencing industry best practices to bolster credibility.

The main goal of this research is to create evidence-based practice guidelines that are specifically designed for public administrations to implement. These rules provide a means of smoother interactions between corporations, governments, and citizens, while also clearing the path for more effective government operations. Governments can utilize blockchain technology to improve decision-making, build citizen confidence, expand options for engagement, and strengthen accountability and transparency.

KEYWORDS

e-Government, Smart Democracy, Consortium Blockchain; Off-chain transactions

Sustainable Development Goals (SGD):

INDEX

LIST OF FIGURES

LIST OF ABBREVIATIONS & ACRONYMS

IT	Information technology
BCT	Blockchain technology
CBC	Consortium blockchain
DSR	Design science research
DLT	Disctributed ledger technology
SC	Smart Contracts
ZKP	Zero Knowledge Proof

1 INTRODUCTION

1.1 BACKGROUND AND PROBLEM IDENTIFICATION

There are several problems facing civilization today, including as the COVID-19 pandemic's economic effects, racial injustice, climate change, and wealth disparity. (Mattar, S. D., Jafry, T., Schröder, P., & Ahmad, Z. , 2021). The goal of public administrations is to address these problems and guarantee that all individuals have access to the resources they require through the development of policies, initiatives, and programmes. This covers funding for activities related to renewable energy, infrastructure, education, and public health. Furthermore, a great deal of public administration is attempting to ensure that all people' opinions are heard and to advance diversity and inclusion. (McCandless, S., Bishu, S. G., Gómez Hernández, M., Paredes Eraso, É., Sabharwal, M., Santis, E. L., & Yates, S., 2022). People want their government to protect and uphold their rights to privacy, security, and human rights. They want a fair and unbiased legal system, access to effective remedies and justice, equitable access to government services, and access to adequate healthcare and education. They also want government officials to be held accountable for their actions, transparency and openness in government operations, and public safety and security through prevention and emergency response investments.

E-government deployment is a complicated process, and problems continue to arise even in places that meet the requirements. Governments and companies are now required by the Information Technology (IT) revolution to offer more effective and secure online services. Dien Novita's research has revealed ongoing problems with South Sumatra's e-government implementation, which has left the public unaware of the benefits and uses of the province's e-government programmes. Increasing the efficacy of e-Government through the use of new technologies is crucial in order to address this problem. Adopting blockchain technology, which provides five essential features for enhancing e-Government—simplicity, digital verification, data sharing, enhanced public security, and cost-effectiveness—is the answer. This study offers a conceptual framework and techniques to support the long-term growth of e-Government in South Sumatra. (Febriansyah, D., Antoni, D., & Lestari, E., 2020)

Over the past ten years, blockchain technology, or BCT, has attracted attention from all over the world. It was first presented as the basis for cryptocurrencies such as Bitcoin. But as knowledge grew, it became clear that blockchain's potential went beyond cryptocurrencies and affected sectors like government, banking, and healthcare.

Blockchain is essentially a peer-to-peer, decentralised network in which users approve and oversee transactions. It is made up of linked blocks, each of which has transaction data that has been encrypted using cryptographic techniques. Consensus, distributed computation, immutability, and authentication are among the main characteristics of blockchain.

Blockchains have several uses: public blockchains are accessible to everyone, private blockchains are only accessible to verified users, and consortium blockchains include aspects of both. Its operating model must be understood in order to be implemented in many fields. Difficulties include scalability, legal compliance, privacy and security concerns, early infrastructure expenditures, and the requirement for specialised knowledge. (Komalavalli, C., Saxena, D., & Laroiya, C., 2020)

While the application of blockchain technology in public administration appears promise, it is unclear how best to deploy it or what applications would work best. (Xu, C., Yang, H., Yu, Q., & Li, Z., 2019). This issue leads to the formulation of the following research question:

RQ: Which will be the recommended blockchain based architecture for Public Administration?

1.2 OBJECTIVE

The purpose of the research is to offer a blockchain-based data sharing architecture for public administration that supports smart contracts, operational security, security policies, and diverse data in an effort to address the research issue that has been posed.

In this dissertation, an architecture for public administration will be developed using the Consortium blockchain (CBC), with a focus on improving data transactions and preserving security in all relevant domains.

To accomplish the research aim, the subsequent intermediate goals were established:

- Make a comprehensive study on blockchain e-government implementation;
- Identify which important architecture measures are needed to discourse and how architecture will be created;
- Define the rules and policies of government and public administrations means which things they allow to be in the public domain and which should be private;
- Propose a blockchain based architecture;
- Validate the Architecture;

1.3 IMPORTANCE AND RELEVANCE

Blockchain is essential to the public sector; the abstract emphasizes how important it is in many ways. It is becoming more widely acknowledged in academic literature as a technology that has the potential to completely transform governance. This is demonstrated by the first comprehensive assessment of the literature that covers blockchain's applications in all major public services, demonstrating the technology's wide-ranging impact on a range of governmental functions. Significant benefits are anticipated for governments, particularly in the areas of increased efficiency and traceability, which can result in better governance. The assessment does, however, also recognize the dangers and difficulties associated with the use of blockchain technology, highlighting the necessity of a comprehensive grasp of its ramifications and designating it as a government strategy. The possible effects on federal personnel also underscore the significance of blockchain by highlighting its ability to lower bureaucracy and enhance agency collaboration. Blockchain helps citizens feel more confident about e-Government initiatives by ensuring greater security and transparency in government interactions. The technology's focus on data security highlights how important it is to protect private and sensitive citizen information while upholding public confidence.

Furthermore, the potential of blockchain technology to save expenses and stimulate innovation bears significant consequences for resource optimisation and service modernization. International cooperation in blockchain projects emphasises the technology's significance on a global scale and suggests how cross-border knowledge sharing could use blockchain to improve governance. In summary, blockchain is a technology that has significant consequences for contemporary governance and that both governments and researchers need to pay attention to. (Cagigas, D., Clifton, J., Diaz-Fuentes, D., & F. Marcos, 2021)

In the digital era, consortium blockchain technology appears to be a vital answer to the urgent security and privacy issues that e-government systems must deal with. Consortium blockchains offer a strong foundation for protecting sensitive data about individuals, companies, and government entities, while traditional, centralised systems are vulnerable to data leaks and hacks. Consortium blockchains, as opposed to public blockchains, offer a degree of confidence that public blockchains are unable to match by involving a small number of pre-approved entities in consensus and decision-making. This regulated method improves data integrity and

security by efficiently validating transactions and guaranteeing that only authorised users can access the network. E-government systems can greatly increase information exchange and openness while defending against security risks, which are an increasing worry in our connected digital world, by utilising consortium blockchains. Furthermore, consortium blockchain technology gives e-government applications more scalability and efficiency. It makes it easier for government agencies and departments to work together and makes it possible for trustworthy parties to securely exchange information. By limiting network participation, this method also reduces the possibility of a 51% security assault, a flaw in public blockchains. Consort blockchain technology is being incorporated into e-government systems in line with the global shift towards transparent, decentralised, and secure digital governance. This move will protect sensitive data while enhancing the efficacy and efficiency of government services. (Elisa, N., Yang, L., Li, H., Chao, F., & Naik, N., 2020)

2 LITERATURE REVIEW

2.1 EMERGING BLOCKCHAIN TECHNOLOGIES AND APPLICATIONS IN GOVERNMENT

One type of distributed ledger technology (DLT) that makes safe and quick data sharing and transaction processing amongst multiple organizations possible is the consortium blockchain. As a way to save costs and streamline processes, government organizations are becoming more and more drawn to technology.

Digital identity management is one of the most widely used applications of Consortium blockchain in government. In this regard, Bouras, Lu, Dhelim, and Ning (2021) offer a simple and novel solution that makes use of consortium blockchains to handle the complex problem of identity management in the Internet of Things (IoT) ecosystem. The authors present a scalable, safe, and decentralized identity management system that emphasizes the registration, authentication, and revocation procedures. They have made a significant contribution to the field of identity management in the Internet of Things with their architectural framework and protocols. By putting their strategy into practice with Hyperledger Fabric, (Bouras, M. A., Lu, Q., Dhelim, S., & Ning, H., 2021)validate its efficiency and efficacy, emphasizing the significance of blockchain-based solutions in this dynamic domain. Important new information about the use of consortium blockchains for IoT identity management in government settings is provided by this study.

Smart contracts (SC) are another important area where blockchain technology is being applied. These contracts are a ground-breaking development in the automation and carrying out of contracts between several parties. These SC are set to revolutionize traditional contract procedures by utilizing the inherent capabilities of blockchain technology, providing previously unheard-of levels of efficiency, security, and transparency. Due to the lack of middlemen, these self-executing contracts made possible by blockchain lower the price and duration of contract fulfilment. Furthermore, SC function according to predetermined guidelines, guaranteeing strict adherence and reducing the possibility of disagreements or violations. Because every transaction is recorded on the blockchain ledger with unchangeable accuracy, transparency is ingrained and fosters confidence among all participants. With the unwavering certainty of blockchain-backed SC, contractual procedures can be expedited and strengthened in a variety of industries, including supply chain management and financial services. (Xiong, W., & Xiong, L., 2020)

Governments can use this technology to safely communicate data across several departments and agencies by using CBC for data sharing. Since data is only transmitted when necessary and can be managed and audited in real time, this can help enhance efficiency and streamline procedures.

Government use of CBC is growing in popularity as a cost- and process-saving measure. Among other things, data sharing, SC, and digital identity management can all benefit from its use. Future use of the technology by more government bodies is likely as it develops.

2.2 BLOCKCHAIN IN GOVERNMENT

2.2.1 BLOCKCHAIN-ENABLED GOVERNMENT: CURRENT AND FUTURE USES

The idea of blockchain-enabled government is becoming more and more popular among public officials. Governments are investigating ways to increase service security, transparency, and efficiency through distributed ledger technology. It is possible to strengthen the security of official documents by using CBC. Encryption and digital signatures allow governments to guarantee the security and immutability of their records. Furthermore, safe voting procedures and easier legal document authentication can be achieved with blockchain-enabled governance. (Zhang, 2023)

The Estonia e-Estonia project currently uses a blockchain consortium platform that enables citizens to securely access and control their data. A distributed ledger that houses and exchanges information about individuals and companies, including tax returns, medical records, and company registration details, makes up the platform. Citizens can also safely access digital services like e-voting, digital IDs, and digital signatures using the platform. This particular technology has been effectively employed for online voting in Estonia and is presently being utilised in other nations, including the United Kingdom. In the future, the platform might be utilised to create new applications like distributed autonomous organisations, which might completely change how governments communicate, as well as safely store and exchange health records.

Governments have a fantastic potential to enhance the security, openness, and effectiveness of their services through the usage of blockchain-enabled governance. It's possible that new services and applications will surface as governments investigate the potential of blockchain-

enabled government. In the end, the application of blockchain technology to government is a positive step forward for the public sector. (Ning, X., Ramirez, R., & Khuntia, J., 2021)

2.2.2 THE IMPACT OF CONSORTIUM BLOCKCHAIN ON GOVERNMENT: BENEFITS, RISKS, AND REGULATORY CONSIDERATIONS

Increasing transparency, increasing efficiency, and enhancing security are just a few advantages that the use of a consortium blockchain holds for government operations. But, it's crucial to take into account the possible hazards of putting in place a consortium blockchain, including its complexity, cost, and potential impact on current laws and regulations. To guarantee a consortium blockchain's effective deployment, governments ought to take into account the ramifications for privacy and security, sufficient supervision, and any influence on current rules. By doing this, you can minimize any risks and guarantee that the consortium blockchain can provide the desired benefits.

2.2.3 IMPLEMENTING BLOCKCHAIN IN GOVERNMENT: STRATEGIES FOR SUCCESS

Blockchain technology offers several advantages for government operations, which is why governments and agencies worldwide are increasingly implementing it. (Fresneda, J., & Sánchez, D., 2020). Blockchain technology is being used by governments more and more to lower expenses, improve operational efficiency and transparency, and give individuals safe access to data. (Gervais, A., Karame, G.O., Wüst, K., & Glykantzis, V., 2016)

Governments should design their implementation strategies strategically in order to guarantee the successful adoption of blockchain technology. This entails figuring out use cases, analysing the legal and regulatory environment, figuring out the dangers connected to the technology, and putting out an extensive roadmap.

Governments should think about the areas where blockchain can have the greatest impact when selecting which use cases to concentrate on. Blockchain, for instance, can be used by governments to protect confidential information, expedite approval procedures, and lower fraud. Blockchain technology can also be used by governments to give people safe access to public services like voting, healthcare, and education. (Batubara, F. R., Ubacht, J., & Janssen, M., 2018)

Governments should make sure that their implementation plans for blockchain technology comply with all applicable rules and regulations in terms of the legal and regulatory landscape. This entails being aware of all current legal requirements as well as any future ones that might be necessary in order to apply blockchain technology. (Ølnes, S., & Jansen, A., 2017)

Governments and agencies may guarantee the success of their blockchain initiatives by adopting a strategic approach to the technology. Governments may make sure that their blockchain projects are effective and benefit their population by finding use cases, analysing the legal and regulatory environment, assessing the risks connected with the technology, and developing a thorough roadmap.

2.2.4 BLOCKCHAIN ADOPTION AND DEPLOYMENT FOR GOVERNMENT:

Government consortium blockchain is an effective instrument for changing the way the public sector functions. It makes it possible for governments to offer their constituents and other stakeholders safe, open, and effective services. Governments may boost transparency, cut expenses, and streamline operations by putting in place a consortium blockchain.

The idea of a distributed ledger must be understood in order to comprehend how consortium blockchains operate. A distributed ledger is a technology that facilitates the safe, decentralised storing, sharing, and management of data. It allows users to view, share, and save information safely and securely without the assistance of a third party.

One kind of distributed ledger that is shared and kept up to date by numerous parties is the consortium blockchain. Typically, these players consist of individuals, private groups, and governments. Every participant has equal access to the data and can edit it as needed. (Naz, M., Al-zahrani, F. A., Khalid, R., Javaid, N., Qamar, A. M., Afzal, M. K., & Shafiq, M., 2019)

In contrast to other distributed ledger systems, the consortium blockchain enables efficient, safe, and transparent stakeholder collaboration. SC, which may be used to automate business procedures and enforce agreements amongst various parties, are utilised to do this. (Christidis, K., & Devetsikiotis, M., 2016)

Furthermore, the consortium blockchain offers a safe environment for exchanging and storing data. Governments can now safely keep and distribute sensitive data to their constituents thanks to this. (Piao, C., Hao, Y., Yan, J., & Jiang, X., 2021). Moreover, assets and transactions can be tracked and traced via the consortium blockchain.

Government oversight, maintenance, and proper security of the consortium blockchain are necessary to guarantee its security. Along with making ensuring the data is unchangeable and impenetrable, it should also guarantee that all parties may access it safely.

Blockchain consortium technology has the potential to revolutionise public sector operations. Governments can lower expenses, improve transparency, and streamline processes by implementing the technology. Additionally, private information can be safely shared and stored with stakeholders via the consortium blockchain. In the end, governments trying to update their processes will find the consortium blockchain to be a very useful instrument. (Issa, W., Moustafa, N., Turnbull, B., Sohrabi, N., & Tari, Z., 2023)

2.2.5 REGULATORY CONSIDERATIONS FOR CONSORTIUM BLOCKCHAIN

Along with the advantages and dangers that government agencies face from consortium blockchain technology, there are other regulatory issues that need to be resolved. It is imperative for governments to guarantee that their blockchain systems conform to all relevant legal statutes and regulations. Governments also need to make sure that the rules governing the usage of consortium blockchains are enforced and that clear guidelines are established.

Governments must also take into account the possible effects of consortium blockchain technology on data security and privacy. Since consortium blockchains are usually public, anybody can view the data they store. Consequently, it is imperative for governments to guarantee the appropriate security of data kept on consortium blockchains and the protection of individuals' personal information.

The adoption of consortium blockchain technology poses several advantages, hazards, and regulatory considerations for governments (Varshney, S., Vats, P., Choudhary, S., & Singh, D., 2022). Prior to adopting consortium blockchain technology, governments should carefully weigh these considerations and make sure they have the knowledge and resources needed to handle the system efficiently.

2.2.6 BEST PRACTICES IN INDUSTRIES OF CONSORTIUM BLOCKCHAIN

For consortium blockchain projects, putting in place a solid governance framework is essential. By doing this, it should be possible for choices to be decided by consensus and for all participants to have a voice. Establishing unambiguous roles and responsibilities for consortium members is crucial in guaranteeing that all parties are cognizant of their respective

responsibilities and obligations. To guarantee that the network is safe, dependable, modular, and expandable, suitable technological solutions must also be chosen. Strong security mechanisms, including protocols for encryption, authentication, and authorization, should be put in place to guarantee the network's security. To guarantee interoperability amongst various parties, a standardised framework should also be built. All transactions should be accessible and verifiable, and there should be explicit dispute resolution procedures in place to guarantee accountability and openness. In order to pinpoint areas for development and guarantee the project's long-term success, it is also critical to track and assess the performance of consortium blockchain projects. Consortium blockchain projects can be effective and leave a lasting impression on the industries they serve by adhering to the above-mentioned recommended practises. (Paul, T., & Rakshit, S., 2022)

2.3 SYSTEMATIC LITERATURE REVIEW ON BLOCKCHAIN BASED ARCHITECTURE

In order to examine the state-of-the-art of CBC research in the area of e-governance, this report used a systematic literature review (SLR). To find, examine, and assess the available empirical studies, research topics, or an interesting phenomenon, the SLR employs the PRISMA technique, as recommended by (al. M. e., 2009), Identifying knowledge gaps, promoting the need for additional research on unexplored concepts, and bolstering the credibility of research efforts and findings are the objectives of this methodical approach. The methodological approach comprises the following main steps: resource identification, selection analysis, data extraction, and data synthesis with findings discussion. Using the PRISMA (Preferred Reporting Items for Systematic reviews and Meta-Analysis) methodology, this SLR will be compiled into a report.

2.3.1 PRISMA SETUP

Identification: Identification: A preselection of pertinent publications will be found by using particular inclusion criteria in order to pursue the primary study objective. In order to avoid using out-of-date research, the time period between 2020 and 2022 was selected with an emphasis on the most recent scholars. Based on the earlier literature analysis, the search phrases comprised in the strings are:

The phrases "public administration" or "public sector" and "blockchain" or "blockchain technology" or "distributed ledger technology" are added, along with the terms "e-Governance" or "e-Government" or "e-Gov") AND ("Consortium Blockchain" or "Consortium Blockchain Technology" OR "Distributed Ledger Technology").

The main sources of information utilised in the search were IEEE Xplore's information systems and technology databases, Science Direct, and general research databases. For this study, additional resources like JSTOR, SSRN, and cross-references should be taken into account as a secondary source.

Screening: Finding evidence of blockchain technology's use to innovative public administration is the aim of this study. Consequently, pertinent publications published during the allotted time period were incorporated into the analysis, whilst those that did not align with the study's scope or primary goal were eliminated.

2.3.2 PRISMA EXECUTION

Finding and eliminating any possible duplicates was the first step in beginning the records analysis. The records were then examined in light of the inclusion criteria. The main text of the articles was reviewed, examined, and summarised in order to make a final selection for the study when the remaining articles appeared to be pertinent to the dissertation goal.

A total of 155 articles were found after the identification of the primary and secondary resources. These included 20 from ResearchGate, 30 from cross-references, 70 from IEEE Xplore, 15 from the Association of Information Systems, and 20 from Science Direct. 82 articles were eliminated in stage 2 because they appeared twice. Step 3 involved screening the remaining 90 articles in two phases, which led to the removal of 70 more articles. Twelve resources were included in the study as a result of Step 4's evaluation of the main text of the 20 remaining articles for eligibility. Ten items that satisfied all inclusion requirements were found through this filter-based technique

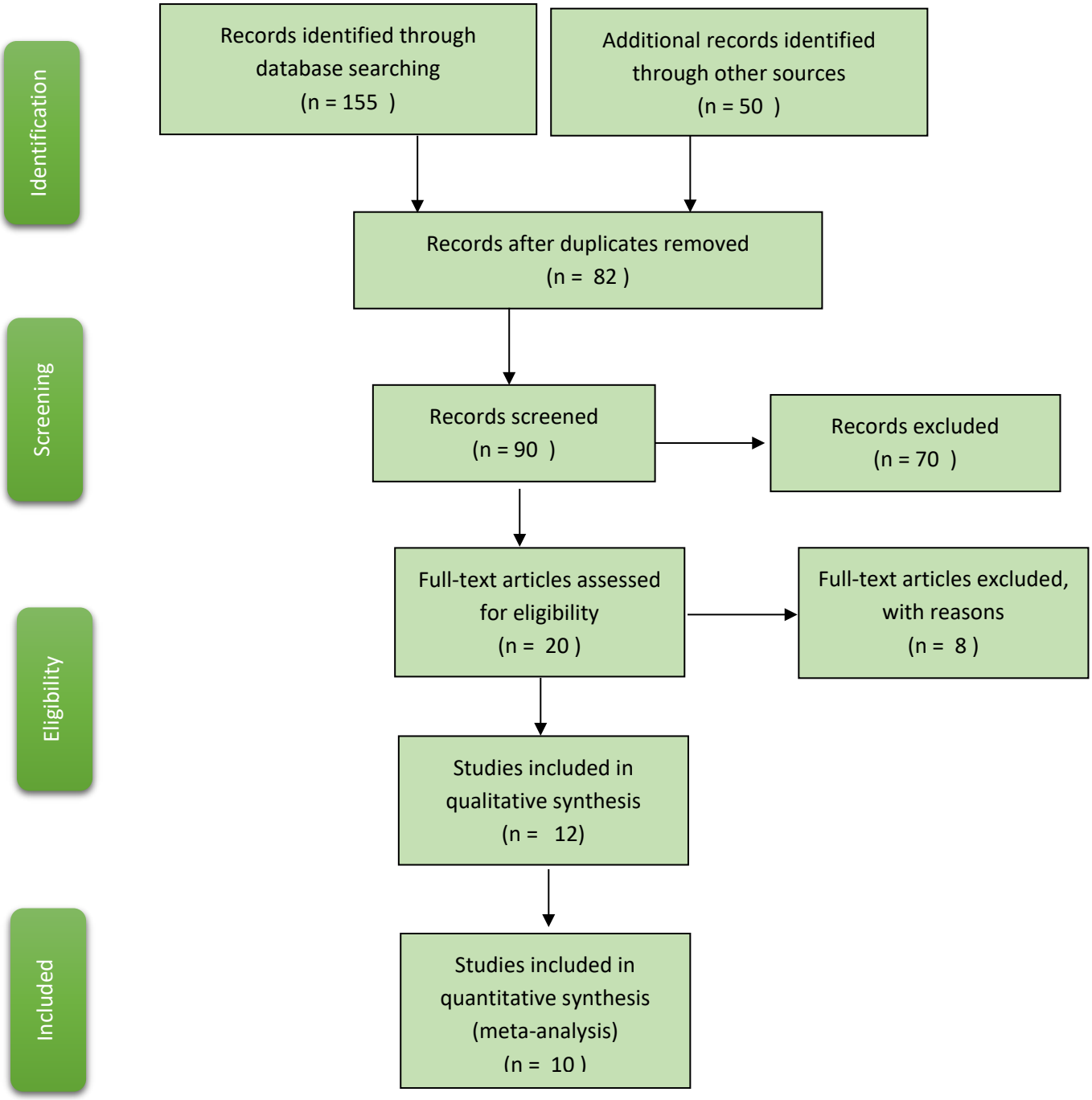

Figure 1: PRISMA Flow Chart

Source; adapted from Moher et.al.; 2009

2.3.3 DISCUSSION

Creating an architecture to close the knowledge gap on consortium blockchain in e-government and smart democracy will be the main goal of this dissertation. The secure transaction protocols, safe data management and storage techniques, and creation of regulatory frameworks to control the application of blockchain technology are all addressed by the suggested design. The use of consortium blockchain will also be emphasised, as a means of facilitating access to public services and data, fostering trust and cooperation between government agencies and the private sector, and facilitating safe and transparent transactions between the latter and the former.
Investigating the complex world of blockchain technology is crucial to the goal of creating a contemporary and efficient blockchain-based architecture for public administration within the framework of e-government and smart democracy. We seek to uncover the possibilities, difficulties, and possibilities that blockchain technology offers to public administration through the examination of ten research papers. As indicated by our research question, "Which will be the recommended blockchain-based architecture for Public Administration?" the main goal of this discussion is to establish the groundwork for a blockchain-based architecture that is in line with the changing requirements of smart democracy and e-government.

REALIZING THE POTENTIAL OF BLOCKCHAIN IN E-GOVERNMENT:

A recurrent issue in the research articles that were reviewed is the potential of blockchain technology to revolutionize public administration and highlight how blockchain can change the way public services are delivered and governed, particularly in the context of smart cities where it can improve security and transparency. Likewise, as highlighted by (Paintner, 2021) blockchain has the ability to improve e-governance's efficiency, transparency, and data security. This potential is further supported by Nishat's report (Nishat, E-Government: Antecedents to Technology Adoption and Creating Public Value in Pakistan., 2022) which emphasizes how blockchain can encourage the use of new technologies in public administration, which will ultimately result in the creation of public value. This collection of studies highlights how blockchain technology might improve e-governance systems' trustworthiness, openness, and data security while meeting the changing demands of public administration.

NAVIGATING THE IMPLEMENTATION CHALLENGES:

There are a number of obstacles in the way of implementing blockchain in public administration, though. Dib and colleagues (Dib, O., Brousmiche, K.L., Durand, A., Thea, E., & Ben Hamida, E., 2018) bring up important issues such as the technical complexity, scaling challenges, and the need for regulatory frameworks and risk mitigation. This sentiment is echoed by Khanna et al., who point out that scalability, regulatory uncertainty, and the need for tangible answers are among the hurdles. According to (Taş, R., & Tanrıöver, Ö. Ö., 2020) security and scalability are the two biggest obstacles to using blockchain technology for electronic voting.

LEVERAGING OPPORTUNITIES FOR IMPROVED GOVERNANCE:

Despite these obstacles, blockchain technology presents a multitude of prospects for improved public administration governance. (Escobar, F., Santos, H., & Pereira, T., 2023) support the use of blockchain technology to simplify and secure data management in identity and records systems for the public sector. Taş and Tanrıöver highlight a number of benefits, such as increased security, lower costs, transparency, and anonymity in e-voting. Theodorou and Sklavos highlight the advantages of enhanced trust in digital interactions, data privacy, secure digital identities, and transparency. In smart cities, there is promise for secure data management, efficient access, and increased collaboration, as highlighted by (Landsbergen, D., Girth, A., & Westover-Muñoz, A., 2022) underscore the potential for secure data management, efficient access, and amplified collaboration in smart cities investigates in more detail how blockchain technology might be used to improve data security, reduce corruption, and increase accountability in the public sector. When used wisely, these prospects support the goal of better public administration in the digital era by promoting accessibility, transparency, and confidence.

Consequently, in light of these revelations, the development of a suggested blockchain-based architecture for public administration ought to thoroughly tackle the pointed-out difficulties while capitalizing on the multitude of prospects. To assure the construction of a safe, open, and effective e-governance system, this design needs to address regulatory considerations, and public awareness. Through leveraging the benefits of data security, anonymity, openness, and efficient data management, public administration may improve accessibility, accountability, and confidence. This suggested design offers a strong basis for the development of public

administration in the digital age and is well-positioned to mesh with the rapidly changing e-government and smart democracy scene."

The following areas will be the focus of the research in order to develop an efficient architecture. The architecture must first guarantee security of the underlying technology and safe transaction protocols, data storage, and management techniques. Second, the design must take into account the creation of regulatory frameworks to control the application of blockchain technology. Third, the architecture must investigate the ways in which consortium blockchain might promote cooperation and trust among citizens, businesses, and government agencies. Fourth, the study must take into account how consortium blockchain might be used to facilitate access to data and public services. Finally, the study must investigate how safe and transparent interactions between the public and government agencies can be.

These are the papers utilized in formulating the architecture development:

S. No	**Title**	**Publish through**	**DOI/Link**
1	Blockchain-Based Security and Privacy in Smart Cities	ScienceDirect	https://doi.org/10.1016/B978-0-12-815032-0.00003-2
2	Blockchain in government: Benefits and implications of distributed ledger technology for information sharing	ScienceDirect	https://doi.org/10.1016/j.giq.2017.09.007
3	Different types of government and governance in the blockchain	Other	https://doi.org/10.22495/jgrv10i1art1
4	Blockchain-Enabled Corporate Governance and Regulation	mdpi	https://doi.org/10.3390/ijfs8020036

5	Blockchain-Enabled Smart Grid Applications: Architecture, Challenges, and Solutions	mdpi	https://doi.org/10.3390/su14148801
6	Blockchain Technology for Improving Transparency and Citizen's Trust	SpringerLink	https://doi.org/10.1007/978-3-030-73100-7_52
7	Blockchain's roles in strengthening cybersecurity and protecting privacy	ScienceDirect	https://doi.org/10.1016/j.telpol.2017.09.003
8	Data Trading Certification Based on Consortium Blockchain and Smart Contracts	IEEE	https://doi: 10.1109/ACCESS.2020.3047398.
9	Trusted and Flexible Electronic Certificate Catalog Sharing System Based on Consortium Blockchain	IEEE	http:// doi: 10.1109/ICCC47050.2019.9064284.
10	Decentralizing Privacy: Using Blockchain to Protect Personal Data	IEEE	http:// doi: 10.1109/SPW.2015.27.

3 METHODOLOGY

In order to achieve the suggested goals, a methodical approach that offers guidance is required in the final proposal for a blockchain-based data sharing architecture for public administration. Because an architecture is an artefact, it is important to keep in mind that a process created especially for creating artefacts is required. Because of this, Hevner & Chatterjee's (2010) research framework and Peffer et al. (2006)'s step-by-step directions for the research approach were used in the Design Science Research technique that was ultimately selected.

3.1 DESIGN SCIENCE RESEARCH

"A problem-solving paradigm that seeks to enhance human knowledge via the creation of innovative artefacts" is the definition of Design Science Research."(Brocke et al., 2020).

Our research on the use of consortium blockchain technology in public administration, namely in the context of e-government and smart democracy, is based on Design Science Research (DSR). DSR is a well-known research approach that creates and assesses novel artefacts to effectively address challenging real-world issues. In our work, the goal of DSR goes beyond improving the status quo; it also attempts to offer workable answers to contemporary problems in the field of smart democracy and e-government research.

As part of this DSR project, a variety of artefacts have been produced, such as models, constructions, theories, techniques, and technological guidelines about design. In addition to augmenting the existing body of knowledge, these artefacts are vital for helping develop workable and useful solutions.

One primary goal is to effectively disseminate knowledge among professionals and academics in the domains of smart democracy and e-government. The generation of information is made valuable and accessible to a wide range of people when theoretical concepts are bridged to their practical application.

Peffers states that DSR consists of six primary activities, which are depicted in Figure 2.

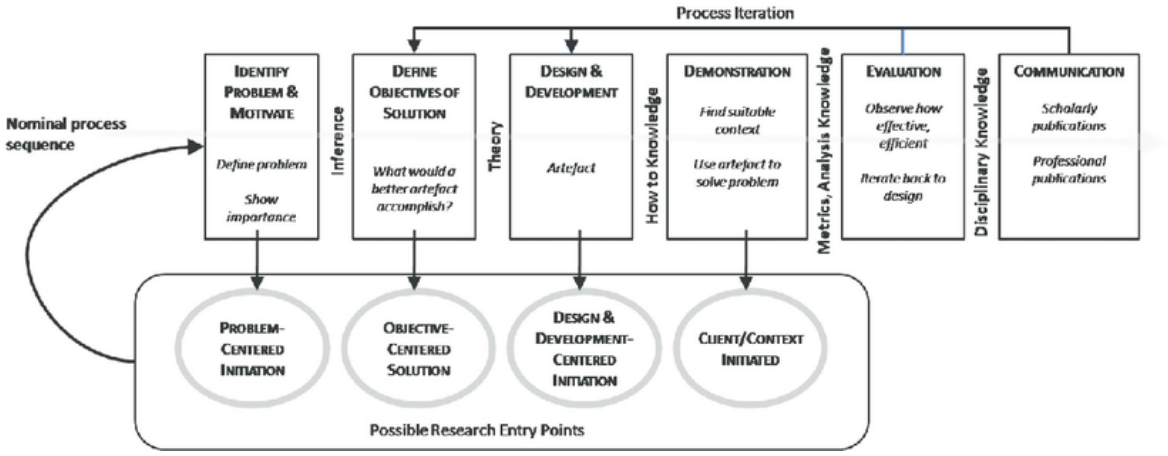

Figure 2 - DSR Methodology Process Model

(Peffers et al., 2008)

3.2 METHODOLOGICAL APPROACH

The Six essential phases make up the DSR model, according to Peffers et al. (2007). Below is a description of these phases:

1. Problem Identification and Motivation: Finding a real-world issue that highlights a research gap is the main goal of the first phase. The chosen problem must be relevant in a larger context and have well-defined reasons for being solved.

2. Objective(s) Definition: This phase builds on the problem identification by specifying the exact goals that must be met in order to create a new IT artefact. These goals must to be based on knowledge acquired during the problem identification stage as well as on earlier research that offers room for improvement or redesign.

3. Design and Development: This stage involves the actual creation of the IT artefact. This phase's strategy is adaptable and created to best serve the specific kind of artefact being made. Both recent findings and body of knowledge are useful in this period.

4. Demonstration: The artefact needs to be tested in a suitable setting after it has been designed. Evaluating its usefulness in solving a practical issue is the goal.

5. Evaluation: Measuring the efficacy and efficiency of the artefact requires completing the evaluation step. Input from subject matter experts and pertinent sources is obtained to inform any necessary redesigns or revisions. An iterative procedure that could return to the design and development phase is made possible by this phase.

6. Communication: Research findings are shared through results publication in the last stage. The overarching goal of this step is to add to the body of knowledge and make the IT artefact usable in real-world scenarios. It also motivates other researchers to analyse the results and think about making changes.

3.3 METHODOLOGICAL APPROACH USED IN CURRENT RESEARCH

The Design Science Research (DSR) model adoption is critical to the advancement of knowledge and innovation in the fields of smart democracy and e-government. For the purpose of creating and validating IT artefacts that attempt to solve real-world problems, the DSR model offers an organised and iterative process. In this environment, our study sets out to transform citizen-government relations and usher in a new era of intelligent democracy. The first step in this journey is to identify and motivate the problem. Here, we aim to pinpoint a real-world issue that has both a research gap and practical significance. The chosen issue should make sense in a larger perspective and provide compelling reasons for being solved. Our thesis is motivated by the search for novel ways to improve the effectiveness, openness, and security of public services and government operations as we delve into the nuances of this stage.

The research is conducted in six phases, which are as follows:

1. PROBLEM IDENTIFICATION AND MOTIVATION

The first step of the study process involves identifying a practical issue in the fields of smart democracy and e-government. This issue relates to the requirement for more safe, effective, and transparent public services and government operations, as covered in our thesis. There's no denying that solving this issue would usher in a new era of smart democracy by revolutionising the way governments engage with their constituents. We intend to improve security and privacy, save costs, and streamline processes by utilising consortium blockchain technology, as we cover in our thesis.

2. OBJECTIVE(S) DEFINITION

Expanding upon the identification of problems, the subsequent stage entails specifying precise goals for the creation of an IT artefact. In this instance, the goals stem from the understandings acquired throughout the problem identification stage as well as from earlier studies in the domains of blockchain technology and e-government. Specifically, as outlined in our thesis, one of our goals is to create a consortium blockchain-based e-government architecture with multiple layers. The entire research process is directed by these goals.

3. DESIGN AND DEVELOPMENT

The study moves on to the design and development stage with clearly stated objectives. We develop the consortium's blockchain-based e-government architecture during this phase, which is detailed in our thesis. Our research emphasises the utilisation of both new discoveries produced during the process and the current expertise in blockchain technology, which is why we took a flexible strategy as described above. Because of this flexible approach, we were able to customise the architecture to fit the unique requirements of smart democracy and e-government.

4. DEMONSTRATION

The next stage after designing the IT artefact is to show off its capabilities in a suitable setting. We describe the implementation and testing of the consortium blockchain architecture as described in our thesis. In this step, the architecture's usability in tackling practical e-government issues including enhancing security, transparency, and public service delivery is assessed.

5. EVALUATION

The assessment stage is essential for determining the IT artifact's efficacy and efficiency. As elucidated in our thesis, feedback is obtained from pertinent sources and topic specialists. This input facilitates an iterative process by informing any necessary redesigns or adjustments. In our instance, the review stage was essential to ensuring that the consortium's blockchain-based e-government architecture was optimised for bettering government services and operations.

6. COMMUNICATION

The last stage involves sharing the research findings and making the IT artefact accessible for real-world use. Thus, it emphasises how crucial it is to share the findings of our thesis. This accomplishes the larger goal of adding to the body of knowledge already in existence and motivating other scholars to carefully examine our work and contemplate future developments in the field of e-government and smart democracy.

The approach to tackling the potential problems in the realm of e-government and smart democracy is logical and thorough since the thesis is organized around these six DSR phases.

4 DEVELOPMENT AND PROPOSED ARCHITECTURE

In The purpose of this chapter is to investigate consortium blockchain technology's potential for smart democracy and e-government. It will assess the efficacy and data security of the technology as it stands today and suggest an architecture for putting one of these systems into place. The study will examine the advantages and disadvantages of each strategy for integrating consortium blockchain technology into e-government and smart democracies. To provide a more safe and effective system for e-government and smart democracy, the suggested architecture will also be put to the test to gauge its efficacy and security.

4.1 STAKEHOLDERS IN E-GOVERNMENT AND SMART DEMOCRACY

Consortium blockchain technology is laying the groundwork for a new era of smart democracy and revolutionizing the way government's function. Governments may improve security and privacy while streamlining operations and cutting expenses by utilizing distributed ledger technology. Governments may safely verify and conduct business with a variety of stakeholders, including voting systems, property registries, healthcare and transportation providers, educational institutions, budgeting and taxing authorities, and security and safety agencies, by utilizing consortium blockchain.

As seen in Figure 3, consortium blockchain has several applications in the transportation industry, including regularizing insurance and accident claims, facilitating transactions including vehicle ecosystem data, and monitoring vehicle life. Consortium blockchain can be used in the healthcare industry to improve data security and transparency, harmonies patient information, and foster industry interoperability. Consortium blockchain has applications in education, including digital identity management, transcript verification, and safe storage of student and faculty records. Blockchain consortiums can be utilized for property and inland registration, document verification, fraud detection, and automatic payment processing. Consortium blockchain can be used to decrease redundancy, improve convenience, and stop voter fraud in elections. Blockchain consortiums can be used to simplify tax collection, boost efficiency, resolve conflicts, and improve transparency in budgeting and taxation. Consort blockchain technology can also be used to enhance digital identity management for both locals and foreign nationals, as well as to reduce online fraud.

Governments may establish a safe, effective, and transparent platform for carrying out administrative tasks and offering citizens public services by utilizing consortium blockchain.

This technology is ushering in a new era of smart democracy by transforming the way governments engage with their constituents.

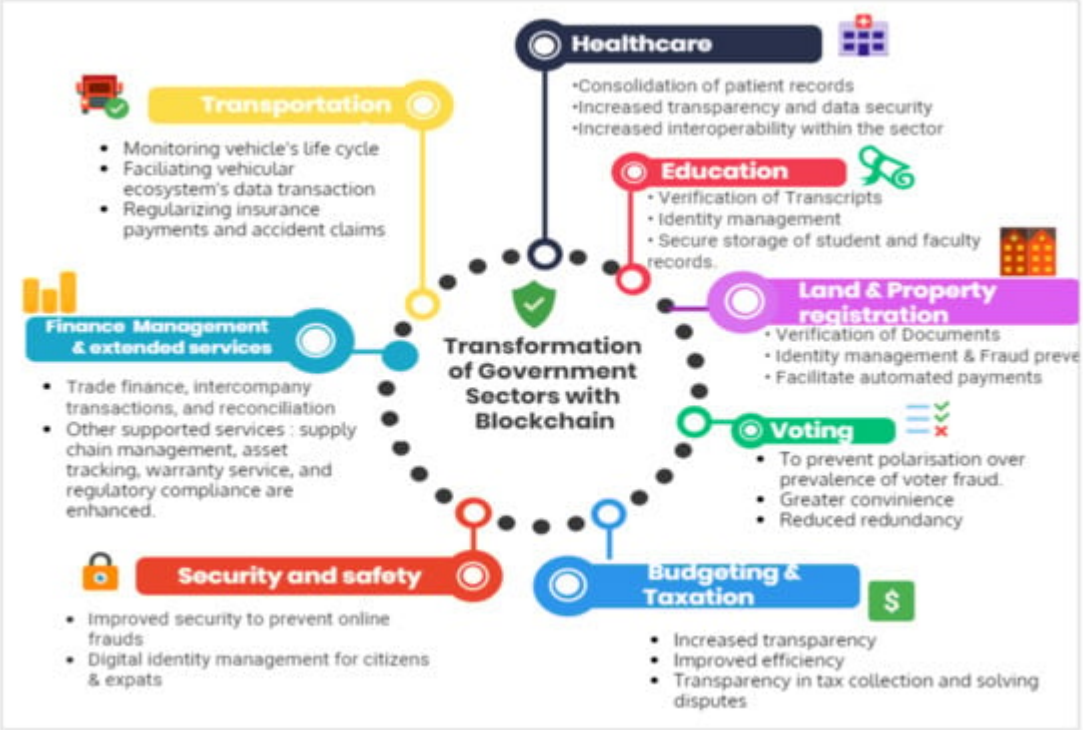

Figure 3 – Transformation of Government

(Khan 2022)

4.2 ASSUMPTIONS

The following presumptions are established in order to fully explore the possibilities of the suggested implementation guidelines, based on the findings gathered from the comprehensive research conducted:

A.1 Establishing Secure Digital Identities and Data Exchange: Consortium blockchains offer a robust solution for creating and maintaining secure digital identities for citizens, institutions, and businesses. This ensures the confidential and protected exchange of data among these entities, enabling secure transactions such as payments, medical records management, and identity document verification.

A.2 Streamlining Automated, Secure, and Cost-Efficient Governance Processes: Leveraging consortium blockchains enables the automation and secure optimization of various governance processes. This includes the seamless exchange of information between government and

citizens, efficient handling of tax filings and fees, and the secure tracking of contracts and payments—all achieved in a cost-efficient manner.

A.3 Enhancing Transparency and Accountability in Government Operations: Consortium blockchains contribute significantly to achieving heightened transparency and accountability within government operations. The technology creates an immutable and tamper-proof record of all activities, ensuring that decisions, processes, and operations are verifiable and transparent to stakeholders.

A.4 Improving Public Service Delivery for Enhanced Efficiency: Consortium blockchains play a pivotal role in securely and efficiently delivering public services, such as healthcare, education, and transportation. Through the secure exchange of data between citizens, institutions, and businesses, including the facilitation of payments and contracts, public services can be streamlined and optimized.

A.5 Ensuring Secure and Reliable Voting Processes: The use of consortium blockchains provides a secure foundation for managing voting processes and the accurate counting of election results. This is achieved through the creation of secure digital identities for voters, the secure storage and counting of votes, and the establishment of an immutable and tamper-proof record of all voting activities.

A.6 Automating Financial Transaction Distribution and Collection: Consortium blockchains provide a safe and automated way to distribute financial transactions, including as taxes, fees, fines, and subsidies. The integrity of data shared between individuals, organizations, and companies is guaranteed by the formation of secure digital IDs for entities.

A.7 Securely Managing and Tracking Public Contracts: Consortium blockchains provide a secure and automated approach to managing and tracking public contracts. By establishing secure digital identities for entities, data can be securely stored and exchanged between citizens, institutions, and businesses, ensuring the integrity of public contracts.

A.8 Automating Management and Tracking of Public Funds: Leveraging consortium blockchains facilitates the secure and automated management and tracking of public funds. This involves creating secure digital identities for entities and securely storing and exchanging data between citizens, institutions, and businesses to ensure the proper use of public funds.

A.9 Securely Managing Public Records: Consortium blockchains offer a secure and automated solution for managing public records. Through the creation of secure digital identities for entities, data can be securely stored and exchanged between citizens, institutions, and businesses, ensuring the integrity and confidentiality of public records.

Also, the Rules and Policies of Govt and Public Administration proposed by (Tan, E., Mahula, S., & Crompvoe, J.) (Kettl, 2016) should be considered:

1. Government and public administration should ensure that all information collected, stored, and disseminated is secure and that the rights of individuals are respected.
2. Government and public administrations should prioritize transparency by making documents, data, and records available to the public in an easily accessible format.
3. Government and public administrations should use appropriate measures to protect the privacy of individuals, including the secure storage and disposal of personal data.
4. Government and public administrations should ensure that any decisions and information released to the public are well-informed and evidence-based.
5. Government and public administrations should be mindful of their legal obligations, including compliance with applicable laws, regulations, and standards.
6. Government and public administrations should develop and maintain policies and procedures to support effective public engagement.
7. Government and public administrations should ensure that the public has access to accurate, up-to-date, and easily accessible information about the policies, procedures, and services they provide.
8. Government and public administrations should provide clear guidance on acceptable uses of public assets and resources, including how they may be used for political purposes.
9. Government and public administrations should ensure that any contracts, grants, or other agreements are properly managed and monitored to ensure compliance with applicable laws and regulations.

10. Government and public administrations should provide training and support to staff to ensure that they understand and adhere to the policies and procedures in place.

4.3 IMPORTANT ARCHITECTURE MEASURES (HOW ARCHITECTURE WILL BE CREATED)

The following elements must be present in the architecture for it to operate correctly. First, large-volume transaction-handling data storage and management techniques, as well as secure transaction protocols, should be incorporated into the design. Second, the architecture needs to incorporate legislative frameworks that control how blockchain technology is utilized, particularly with regard to public services and data. Third, steps to improve cooperation and trust between public sector agencies, businesses, and individuals should be incorporated into the design. Fourth, mechanisms that facilitate secure and transparent transactions between citizens and government agencies should be included in the architecture, as well as access to public services and data. To guarantee that employees comprehend and follow the established policies and processes, the architecture should also have methods for staff support and training.

4.4 PROPOSED ARCHITECTURE

Smart democracy and consortium blockchain technologies form the foundation of the proposed consortium blockchain-based e-government architecture. The consortium blockchain layer, the network layer, the services access layer, and the ledger storage layer make up its four tiers. The services access layer stores user credentials and grants access to computer resources and e-government users across a range of devices. Pre-selected e-government validators form a peer-to-peer network known as the consortium blockchain layer, which is in charge of authenticating new e-government users and confirming transactions. In addition, this layer offers services for user identity management, consensus, and peer-to-peer communication. The e-government consortium blockchain network, the ledger storage, and user connectivity are all guaranteed by the network layer. Images, PDFs, DOCs, contracts, and other off-chain (SideDB) data that are too big to be saved on the blockchain or that may need to be modified or removed in the future are stored in the ledger storage layer. This layer is required since the blockchain database can only be added to and is immutable, meaning that it cannot be deleted in the future. The ensuing subsections go into greater depth about each of these layers.

4.4.1 SERVICE ACCESS LAYER

This layer provides an interface for users to interact with the e-government system. The services provided by this layer include user authentication, document sharing, and other e-government services. To ensure security and privacy, this layer uses zero-knowledge proof algorithm to authenticate users without revealing their identity or sensitive information.

The user interface and point of contact for your consortium's blockchain-based e-government and smart democracy system is the Service Access Layer. It is essential for maintaining user security and privacy as well as for enabling document sharing, user authentication, and access to a range of programmers and services.

FUNCTIONALITY:

1. USER AUTHENTICATION:

ZKP-Based Authentication: Users initiate authentication processes that rely on ZKPs. These proofs allow users to verify their identity or attributes without disclosing sensitive information.

SC Validation: It validates ZKPs provided by users. They check if the proofs meet the required criteria without exposing the underlying data.

Privacy-Enhanced Verification: ZKPs can be used to confirm various attributes like age, citizenship, or eligibility for specific services or voting. For instance, a user can prove they are of voting age without revealing their actual birthdate.

2. DOCUMENT SHARING:

Secure Hash Functions: Document sharing involves the use of cryptographic hash functions. Users' documents are hashed before being shared or stored on the blockchain.

End-to-End Encryption: To maintain confidentiality during transmission, the hashed documents are encrypted with the recipient's public key, ensuring that only the intended recipient can access and decrypt the document.

3. ACCESS CONTROL:

SC Driven Access Rules: ZKPs and user attributes are used by SC to construct access control rules. For instance, in order to use some government services, a user might have to provide proof of citizenship.

Attribute Verification: User characteristics are verified using ZKPs and other privacy-enhancing methods. The user's eligibility for a specific service or procedure is verified by the SC.

4. ERROR HANDLING AND FEEDBACK:

User-Friendly Feedback: The layer provides user-friendly error messages and guidance in case of authentication or access issues.

Troubleshooting Assistance: Users receive clear instructions on how to resolve authentication problems, ensuring a smooth and user-friendly experience.

5. USER INTERFACES:

Intuitive Interfaces: Develop intuitive web or mobile applications that abstract the complexities of blockchain and cryptography for users.

User Guidance: Interfaces guide users through the authentication process, document sharing, and service access, ensuring a user-friendly experience.

PRIVACY MEASURES:

Zero-Knowledge Proofs (ZKPs): ZKPs enable users to prove information without revealing it, safeguarding their privacy during authentication and attribute verification.

SC: While safeguarding sensitive data, SC impose restrictions such as access control.

Hash Functions: Cryptographic hash functions ensure data integrity and confidentiality during document sharing.

End-to-End Encryption: Encryption of shared documents with recipient public keys maintains document confidentiality.

The Service Access Layer plays a pivotal role in ensuring secure and privacy-conscious interactions for users within your e-government and smart democracy system. It acts as a

gateway to the consortium blockchain, preserving user privacy while enabling seamless access to services and processes.

4.4.2 CONSORTIUM BLOCKCHAIN LAYER

The Consortium Blockchain Layer is the central component of your e-government and smart democracy system. It uses a consortium blockchain to handle and store e-government data in a safe manner. Data security and integrity are ensured by a group of reliable nodes that manage this blockchain. Furthermore, as maintaining privacy is of utmost importance, the layer encrypts and stores sensitive data on the blockchain using the zero-knowledge proof process, keeping the content of the data hidden.

FUNCTIONALITY:

1. ZERO-KNOWLEDGE PROOFS (ZKPS):

Enhanced Data Privacy: The layer utilizes ZKPs to encrypt and store sensitive data on the consortium blockchain while keeping the content confidential.

Data Verification: ZKPs allow for data verification without revealing the underlying data, ensuring that information can be confirmed without being disclosed.

2. SMART CONTRACTS (SC):

Privacy-Preserving Logic: SC execute with a focus on data privacy. They automate various processes while maintaining confidentiality.

Transparent Execution: Although data is kept private, the execution of SC remains transparent and verifiable on the blockchain.

3. CONSENSUS MECHANISM:

Trusted Node Consensus: A group of trusted nodes maintains the consortium blockchain, ensuring that only reliable parties participate in consensus.

Data Integrity: The consensus mechanism guarantees the integrity and accuracy of data stored on the blockchain.

4. PRIVACY-ENHANCING ALGORITHMS:

Homomorphic Encryption: This technique allows mathematical operations to be performed on encrypted data, preserving privacy.

Confidential Transactions: Transaction details remain confidential while still being validated by the network.

zk-SNARKs: Complex computations on encrypted data can be performed without exposing inputs, enabling privacy-preserving interactions.

SECURITY MEASURES:

Secure Data Storage: Data on the consortium blockchain is securely encrypted and protected against unauthorized access.

SC Security: It undergoes rigorous security audits and testing to prevent vulnerabilities or exploitation.

Auditability: Comprehensive logs ensure that all transactions and SC executions are auditable and traceable.

INTERACTIONS WITH OTHER LAYERS:

The Consortium Blockchain Layer works closely with the Service Access Layer, executing SC for data management and access control, and employing ZKPs to validate user identities and access credentials.

In order to preserve data integrity and privacy, data processing and retrieval from the Ledger Storage Layer take place inside the consortium blockchain.

INTEGRATION OF PRIVACY AND SECURITY:

To protect sensitive data and maintain the smooth functioning of transactions and SC logic, it is essential to employ privacy-enhancing algorithms, ZKPs, and secure SC.

In the consortium blockchain network, trusted nodes are essential to preserving the security and integrity of data.

As the cornerstone of your e-government and smart democracy system, the Consortium Blockchain Layer protects data security, privacy, and dependable governance procedures by utilizing trusted nodes, cutting-edge cryptography, and privacy-preserving mechanisms. This layer protects the secrecy of the data while enabling the safe management and preservation of private government information.

.

4.4.3 NETWORK LAYER

The Network Layer facilitates safe and effective communication between various nodes, acting as the communication foundation of your smart democracy and e-government system. Peer-to-peer network protocols are used by this layer to guarantee data availability, secrecy, and integrity while it is being transmitted. It uses the zero-knowledge proof algorithm to authenticate nodes without revealing their identity or sensitive data in order to improve security and privacy.

FUNCTIONALITY:

1. PEER-TO-PEER NETWORK PROTOCOL:

Secure Communication: The e-government system's layer establishes direct and secure communication channels between nodes by implementing a peer-to-peer network protocol.

Efficient Data Exchange: Through effective data interchange and latency reduction, the protocol maximizes network performance.

2. ZERO-KNOWLEDGE PROOFS (ZKPS) FOR NODE AUTHENTICATION:

Privacy-Preserving Node Authentication: ZKPs are utilized to authenticate nodes in the network without revealing their actual identity or sensitive data.

Secure Node Interactions: Nodes can prove their legitimacy and eligibility to participate in the network without disclosing personal information.

SECURITY MEASURES:

Secure Data Transmission: Network protocols and encryption mechanisms are in place to guarantee the secure transmission of data between nodes.

Node Authentication: ZKPs are employed to verify the identity of nodes without exposing their sensitive information, ensuring that only trusted nodes participate in the network.

INTERACTIONS WITH OTHER LAYERS:

The Network Layer interacts closely with the Consortium Blockchain Layer, enabling nodes to transmit transactions, SC data, and encrypted documents securely.

It ensures that data from the Ledger Storage Layer is securely transmitted to maintain data privacy and integrity.

INTEGRATION OF PRIVACY AND SECURITY:

Privacy is a paramount concern in the Network Layer. ZKPs protect the identity and data of nodes during authentication, preventing exposure of sensitive information.

Security measures, including encryption and secure protocols, are implemented to safeguard data in transit and prevent unauthorized access.

NODE MANAGEMENT:

Authorization and Authentication: ZKPs are used to authenticate nodes and grant them permission to engage in network activities. By doing this, the communication network is guaranteed to contain only authentic nodes.

Firewalls and Intrusion Detection: To guard the network against illegal access and attacks, security measures like firewalls and intrusion detection systems are installed.

DATA PRIVACY AND INTEGRITY:

Data Privacy: Privacy-preserving protocols and encryption ensure that data transmitted between nodes remains confidential.

Data Integrity: To ensure the integrity of the information transferred, steps are taken to identify and stop data tampering during transmission.

Your smart democracy and e-government system depends on the Network Layer, which offers a private, effective, and safe channel of communication between nodes. This layer guarantees safe data transmission while protecting sensitive data and node identities through the use of a peer-to-peer network protocol and zero-knowledge proofs for node authentication.

4.4.4 LEDGER STORAGE LAYER

The Ledger Storage Layer plays a pivotal role in your e-government and smart democracy system by securely and efficiently storing ledger data. It employs distributed ledger technology to manage data in a tamper-resistant and decentralized manner. To enhance data security and privacy, this layer leverages the zero-knowledge proof algorithm to encrypt and store data securely without exposing the actual content.

FUNCTIONALITY:

1. DISTRIBUTED LEDGER TECHNOLOGY:

Data Management: By using distributed ledger technology, the layer makes sure that data is kept in a decentralized, fault-tolerant manner among several nodes.
Tamper Resistance: The distributed ledger provides tamper resistance, making it difficult for unauthorized parties to alter or manipulate data.

2. ZERO-KNOWLEDGE PROOFS (ZKPS) FOR DATA SECURITY:

Data Encryption: ZKPs are employed to encrypt and store data securely on the ledger without disclosing the actual content.
Privacy-Preserving Data Handling: Data privacy is maintained, as sensitive information remains concealed from unauthorized parties.

SECURITY MEASURES:

Data Encryption: To prevent unwanted access, all data kept on the ledger is encrypted using strong encryption methods.
Access Control: Access to ledger data is strictly controlled through SC and cryptographic mechanisms, ensuring only authorized users can retrieve and modify data.

INTERACTIONS WITH OTHER LAYERS:

The Ledger Storage Layer collaborates closely with the Consortium Blockchain Layer, providing data retrieval and storage services.
It also interacts with the Network Layer to ensure secure and efficient data transmission between nodes and the ledger.

INTEGRATION OF PRIVACY AND SECURITY:

The Ledger Storage Layer's primary goals are security and privacy. ZKPs provide data secrecy and encryption while making sure that only authorized users can view and alter data.
Data is protected from unauthorized access and manipulation by the use of security mechanisms like encryption and access controls.

DATA BACKUP AND REDUNDANCY:

To ensure data availability and integrity, data is backed up and stored redundantly across multiple nodes in the distributed ledger network.

AUDITABILITY AND TRANSPARENCY:

Comprehensive logs and data auditing mechanisms are maintained, ensuring that all changes to the ledger data are recorded and traceable.

DATA INTEGRITY VERIFICATION:

Data corruption and tampering are prevented by mechanisms that check the integrity of the data recorded on the ledger.

EFFICIENT DATA RETRIEVAL:

To enable effective access to ledger data while preserving confidentiality and privacy, indexing and retrieval techniques are used.

The foundation of your smart democracy and e-government system is the Ledger Storage Layer, which makes sure that data is safely kept, impenetrable, and privacy-aware. This layer effectively permits authorized parties to access and interact with the ledger while guaranteeing the confidentiality and integrity of sensitive data through the use of distributed ledger technology and zero-knowledge proofs.

4-LAYERS WORKFLOW:

As it is presented in Figure 4, the proposed architecture is composed by four layers.

Operating within a layered architectural framework yields significant advantages, particularly in intricate systems like consortium blockchain-based e-government and smart democracy platforms. These layers introduce a structured and modular approach to design and implementation, enhancing the system's operational efficiency and ease of maintenance. Each layer assumes a specialized role, allowing teams to focus on specific aspects and optimize their work. Moreover, layers ensure a distinct separation of responsibilities, simplifying issue identification and resolution, the integration of security protocols, and the preservation of privacy measures. This structured framework fosters teamwork, reduces development intricacies, and facilitates the smooth assimilation of emerging technologies or enhancements. In essence, adherence to layered architecture not only bolsters the system's resilience and

security but also streamlines the development process, rendering it more manageable and adaptable to evolving requirements and technological advancements—making it a pivotal consideration for a thesis exploring these systems.

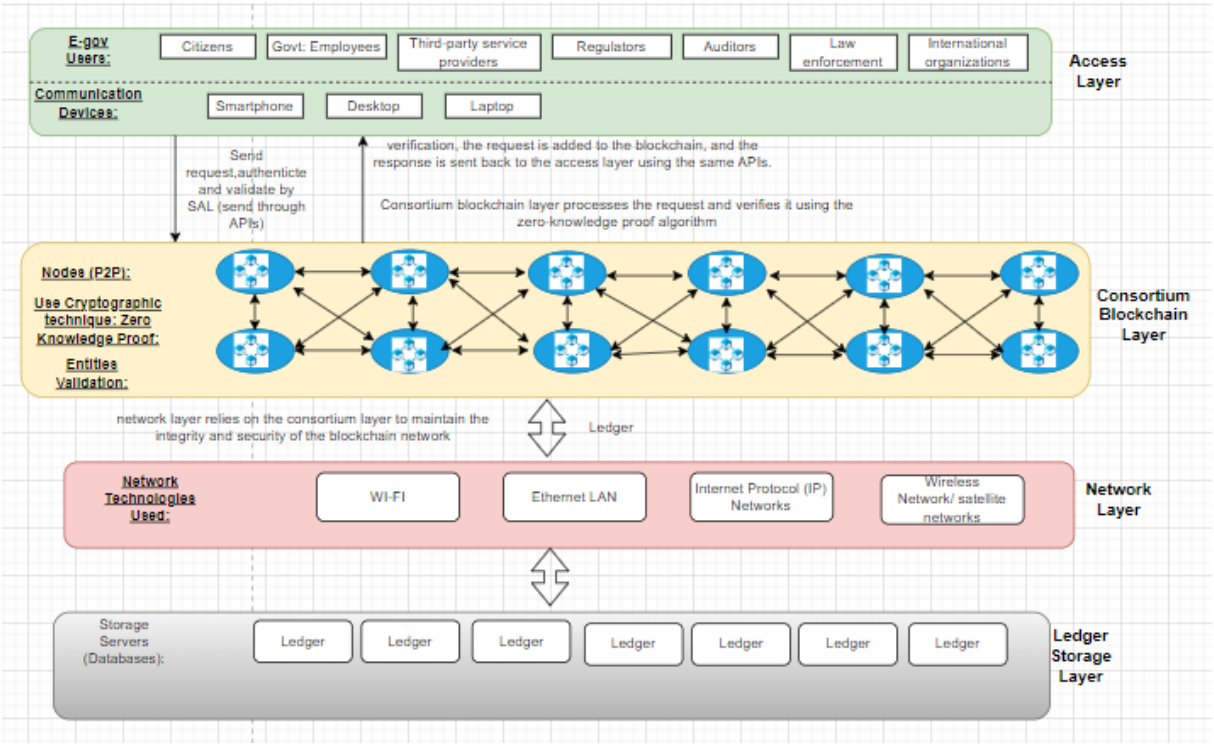

Figure 4: CB Four Layer Architecture 1

5 VALIDATION

Presenting the work to two esteemed experts—Expert 1 and Expert 2—was part of the validation process for the proposed 4-layer architecture in consortium blockchain for e-government and smart democracy. Their analyses were essential in determining the shortcomings of the framework and offering suggestions for its enhancement.

The framework for e-government and smart democracy was presented to Specialists Expert 1 and Expert 2 to start the validation process for the proposed 4-layer architecture on consortium blockchain. The experts were asked three crucial questions after the thorough explanation: first, about the usefulness of the suggested framework; second, about possible objections; and third, about suggestions for its enhancement. By asking these questions, we hoped to get a thorough assessment of the framework's applicability, advantages, disadvantages, and growth opportunities. Insightful answers followed from Expert 1 and Expert 2, who addressed important factors for the framework's successful integration into the domains of smart democracy and e-government, hence influencing the framework's evolutionary trajectory.
Below is a thorough description of the two feedbacks:

5.1 FIRST FEEDBACK:

1) Is the proposed framework useful?

Yes, the proposed framework for e-government and smart democracy using a consortium model and zero-knowledge proofs has some clear advantages:

- **Privacy Protection:** It ensures strong privacy protection for sensitive data like voter identities, which is crucial for e-government and smart democracy.
- **Transparency and Trust:** The use of blockchain, especially in a consortium model, makes government processes transparent and trustworthy. This means that citizens can check transactions and take part in decisions with confidence.
- **Security:** The framework uses the security features of blockchain to prevent fraud and unauthorized access, which boosts overall system security.
- **Efficiency:** By automating numerous procedures, SC cut down on the amount of paperwork and middlemen required, improving the efficiency of government operations.

2) Are there criticisms of the proposed framework?

Yes, there are some concerns:

- **Scalability:** As the system grows and handles more transactions, it might run into scalability problems common to blockchain networks. It's important to address this to ensure the framework's long-term viability.
- **Adoption Challenges:** Implementing a new e-government and smart democracy system requires getting widespread acceptance. Encouraging citizens, government officials, and political entities to switch to this framework could be challenging.
- **Regulatory Compliance:** Ensuring that the framework complies with existing laws and regulations is crucial. Critics might wonder how well the proposed system aligns with current rules and how it adapts to future changes.
- **Operational Costs:** Running a blockchain network can be expensive. Critics may want to understand the costs and whether the benefits justify these expenses.

3) Any recommendations for improving the framework?

To make the framework even better, consider these ideas:

- **Scalability Solutions:** Explore advanced scaling solutions like layer-2 options, sidechains, or sharding to handle more transactions as the system grows.
- **User Education and Adoption Strategies:** Create clear plans for educating and getting users on board, including awareness campaigns, training for government officials, and incentives to encourage participation.
- **Interoperability:** Make sure the framework can work alongside existing systems to make the transition smoother and allow it to coexist with current government processes.
- **Continuous Security Auditing:** Regularly test the system for vulnerabilities through security audits and penetration testing to ensure robust security measures.
- **Feedback Mechanism:** Set up a way to gather input and concerns from citizens and stakeholders to continually adapt and improve the framework.
- **Research on Legal Compliance:** Keep researching and working with legal experts to ensure that the framework remains compliant with changing legal requirements and can adapt to new regulations.

5.2 SECOND FEEDBACK:

1) Evaluation of Framework's Value:

The proposed framework demonstrates substantial value in advancing e-government and smart democracy. The key strengths contributing to its significance include:

Emphasis on Privacy: The framework prioritizes privacy considerations, particularly evident in its approach to digital identities, data exchange, and secure transactions. By integrating privacy-centric features, it aligns with contemporary expectations for safeguarding sensitive information.

Leveraging Blockchain Transparency: Recognizing the inherent transparency of blockchain, the framework adeptly utilizes this feature to enhance various facets of government operations. This strategic use of technology contributes to a more accountable and transparent governance model.

Security Enhancement: The emphasis on security measures, especially through the incorporation of blockchain technology, adds a layer of resilience to the framework. The secure nature of transactions and data management addresses critical concerns related to cyber threats and unauthorized access.

Smart Contracts for Operational Efficiency: The integration of SC introduces a mechanism for streamlining government operations. This automation not only reduces manual intervention but also contributes to increased efficiency in processes like contract tracking and information exchange.

2) Critiques and Considerations:

While acknowledging its merits, the proposed framework is not without its critiques. A comprehensive evaluation of potential challenges includes:

Scalability Challenges: The scalability of the framework may face limitations as user numbers grow. Robust strategies need to be in place to address potential challenges associated with scaling the system for broader adoption.

Adoption Barriers: Identifying and overcoming barriers to adoption is critical for the framework's success. Factors such as user acceptance, training requirements, and change management need to be thoroughly addressed.

Regulatory Compliance: Ensuring alignment with existing regulations and adapting to evolving compliance standards is essential. Regular assessments and updates to accommodate legal requirements will be crucial for sustained success.

Operational Costs: A detailed examination of the operational costs associated with the framework is necessary. Strategies for optimizing these costs without compromising the quality and security of services should be explored.

3) Recommendations for Framework Enhancement:

To further enhance the framework and address identified critiques, the following targeted recommendations are proposed:

Scalability Solutions: Investigate and implement scalable solutions such as sharding or layer-two protocols to accommodate a growing user base effectively.

User Engagement Strategies: Develop and implement robust strategies to enhance user engagement. User-friendly interfaces, educational initiatives, and seamless onboarding processes can contribute to higher user acceptance.

Interoperability Planning: Ensure seamless interoperability with existing government systems. A comprehensive plan for integration will be essential to avoid disruptions and ensure a cohesive digital ecosystem.

Continuous Security Audits: Establish a regular schedule for security audits, with a focus on identifying and addressing emerging vulnerabilities. Proactive security measures are vital for maintaining user trust.

Feedback Mechanism Implementation: Implement a structured feedback mechanism to collect insights from users and stakeholders. Continuous improvement based on feedback ensures the framework remains responsive to evolving needs.

Legal Compliance Monitoring: Develop a systematic approach to monitor changes in legal requirements. Regular updates and adaptations to ensure ongoing compliance will be crucial for the framework's sustainability.

6 CONCLUSION

Following a thorough examination of the body of research and industry best practises, the main hypothesis—that Blockchain (BC) offers a potential technology for improving the public sector—has been verified. Numerous examples of best practises in the public sector across the globe, particularly in the USA, China, Estonia, Switzerland, Dubai, and Switzerland, have shown the many advantages that e-government can offer society.

This thesis demonstrates that a comprehensive framework is required for the application of Blockchain Technology (BCT) in e-Governance through a thorough analysis of pertinent literature. A framework like this should cover the application's breadth, technical and non-technical requirements, stakeholder participation, and observance of crucial compliance procedures. It also has to encourage a cooperative ecosystem in order to guarantee public involvement and optimize the generation of public value.

Experts greeted the suggested framework and related plans favorably, deeming them to be quite beneficial. In order to verify the stability of the framework, a quantitative validation method was utilized. Feedback was carefully considered during this validation process, and minor recommendations for enhancements were added, which helped to strengthen the framework.

6.1 SYNTHESIS OF THE RESEARCH

The methodology followed in this dissertation followed a methodical process. An detailed literature assessment, which was the first step in the research process, demonstrated the value of blockchain technology in the public sector. A thorough assessment of the literature was then carried out, covering both recent industry best practices and scholarly works. The framework for implementing BCT in the public sector was developed based on the combined findings from these processes. Through qualitative expert interviews with people from a range of backgrounds, including industry, government, and academia, the model was validated. The input that was gathered from these interviews helped to improve the first framework, which achieved the stated goals.

6.2 FUTURE WORK

In order to handle increasing user interaction, future development in this area will address scalability issues and concentrate on cutting-edge technologies including layer-2 protocols and sharding. At the same time, user-centric approaches—such as user-friendly interfaces and educational initiatives—seek to increase acceptance, and interoperability planning aims to make the framework function seamlessly with current government systems.

A proactive strategy based on ongoing audits is suggested to strengthen security and guarantee resistance to newly discovered vulnerabilities. The framework's adaptability and compliance in the changing e-governance landscape are further reinforced by the addition of a structured feedback system and continuous legal compliance monitoring.

Bibliography

Batubara, F. R., Ubacht, J., & Janssen, M. (2018). Challenges of blockchain technology adoption for e-government: a systematic literature review. doi:https://doi.org/10.1145/3209281.3209317

Bouras, M. A., Lu, Q., Dhelim, S., & Ning, H. (2021). A Lightweight Blockchain-Based IoT Identity Management Approach. *Future Internet*. doi:https://doi.org/10.3390/fi13020024

Cagigas, D., Clifton, J., Diaz-Fuentes, D., & F. Marcos. (2021). Blockchain for Public Services: A Systematic Literature Review. IEEE. doi:doi: 10.1109/ACCESS.2021.3052019.

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access, 4*. doi:doi: 10.1109/ACCESS.2016.2566339.

Dib, O., Brousmiche, K.L., Durand, A., Thea, E., & Ben Hamida, E. (2018). Consortium Blockchains: Overview, Applications and Challenges. Retrieved from http://www.iariajournals.org/telecommunications/

Elisa, N., Yang, L., Li, H., Chao, F., & Naik, N. (2020). Consortium Blockchain for Security and Privacy-Preserving in E-Government Systems. doi:https://doi.org/10.48550/arXiv.2006.14234

Escobar, F., Santos, H., & Pereira, T. (2023). Blockchain in the Public Sector: An Umbrella Review of Literature. doi:https://doi.org/10.1007/978-3-031-21229-1_14

Febriansyah, D., Antoni, D., & Lestari, E. (2020). The Role of Blockchain Technology in E-Govemment Capability: Literature Review. *2020 Fifth International Conference on Informatics and Computing (ICIC).* IEEE. doi:doi: 10.1109/ICIC50835.2020.9288578.

Fresneda, J., & Sánchez, D. (2020). Blockchain in the public sector: A review of the opportunities for government operations. *Journal of Information Technology & Politics*.

Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Sornette, A. (2016). On the security and performance of proof of work blockchains. *International Conference on Financial Cryptography and Data Security,*. doi:https://doi.org/10.1145/2976749.2978341

Issa, W., Moustafa, N., Turnbull, B., Sohrabi, N., & Tari, Z. (2023). Blockchain-Based Federated Learning for Securing Internet of Things: A Comprehensive Survey. doi:https://doi.org/10.1145/3560816

Komalavalli, C., Saxena, D., & Laroiya, C. (2020). *Overview of Blockchain Technology Concepts.* Academic Press. doi:https://doi.org/10.1016/B978-0-12-819816-2.00014-9

Landsbergen, D., Girth, A., & Westover-Muñoz, A. (2022). Governance rules for managing smart city information. *Information and Software Technology,, 2*(1). doi:https://doi.org/10.1016/j.ugj.2022.05.003

Mattar, S. D., Jafry, T., Schröder, P., & Ahmad, Z. . (2021). Climate justice: priorities for equitable recovery from the pandemic. *Climate Policy*.

McCandless, S., Bishu, S. G., Gómez Hernández, M., Paredes Eraso, É., Sabharwal, M., Santis, E. L., & Yates, S. (2022). A long road: Patterns and prospects for social equity, diversity, and inclusion in public administration. doi:https://doi.org/10.1111/padm.12830

Naz, M., Al-zahrani, F. A., Khalid, R., Javaid, N., Qamar, A. M., Afzal, M. K., & Shafiq, M. (2019). A Secure Data Sharing Platform Using Blockchain and Interplanetary File System. doi:https://doi.org/10.3390/su11247054

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*. doi:https://doi.org/10.1080/02681102.2021.1925619

Nishat, S. (2022). E-Government: Antecedents to Technology Adoption and Creating Public Value in Pakistan. *International Journal of Information Management,*. Retrieved from https://vuir.vu.edu.au/44406/1/NISHAT_Shahid-Thesis_nosignature.pdf

Ølnes, S., & Jansen, A. (2017). Blockchain Technology as s Support Infrastructure in e-Government. doi:https://doi.org/10.1007/978-3-319-64677-0_18

Paintner, P. (2021). Blockchain Technology in the Area of E-Governance – Guidelines for Implementation. *International Journal of E-Government Research,*. Retrieved from https://run.unl.pt/bitstream/10362/123244/1/TGI0433.pdf

Paul, T., & Rakshit, S. (2022). Blockchain-Based Internet of Things: Challenges and Opportunities. doi:https://doi.org/10.1007/978-981-16-9260-4_2

Piao, C., Hao, Y., Yan, J., & Jiang, X. (2021). Privacy preserving in blockchain-based government data sharing: A Service-On-Chain (SOC) approach. doi:https://doi.org/10.1016/j.ipm.2021.102651

Taş, R., & Tanrıöver, Ö. Ö. (2020). A systematic review of challenges and opportunities of blockchain for e-voting. doi:https://doi.org/10.3390/sym12081328

Varshney, S., Vats, P., Choudhary, S., & Singh, D. (2022). A Blockchain-based Framework for IoT based Secure Identity Management. doi:doi: 10.1109/ICIPTM54933.2022.9753887.

Xiong, W., & Xiong, L. (2020). Data Trading Certification Based on Consortium Blockchain and Smart Contracts. *IEEE Access*. doi:doi: 10.1109/ACCESS.2020.3047398.

Xu, C., Yang, H., Yu, Q., & Li, Z. (2019). Trusted and Flexible Electronic Certificate Catalog Sharing System Based on Consortium Blockchain. *2019 IEEE 5th International Conference on Computer and Communications (ICCC).* IEEE. doi:doi: 10.1109/ICCC47050.2019.9064284.

Zhang, W. Q.-A. (2023). Blockchain Technology: Security Issues, Healthcare Applications, Challenges and Future Trends. doi:https://doi.org/10.3390/electronics12030546