Volume XX, Issue (2) (2024) 84-93

International May Conference on Strategic Management

DOI: *10.5937/IMCSM24059S*

Review Article

REVIEW OF SECURITY ISSUES IN THE APPLICATION OF BLOCKCHAIN TECHNOLOGY IN E-GOVERNMENT

Marko Štaka*, Miroslav Stefanović, Darko Stefanović, Đorđe Pržulj, Vladimir Fabri

University of Novi Sad, Faculty of Technical Sciences, Serbia

Abstract: E-government represents a segment of public service modernization. The goal of e-government is to make administrative processes more accessible and easier to use for all citizens. E-government relies on information and communication technologies to improve access and efficiency of services for citizens and the business sector. One of the challenges institutions face for wider acceptance of e-government is distrust that citizens have in online services. For data that is used by e-government services question of data security represents a rather important consideration. Blockchain technology offers a range of advantages in this context, including decentralization, transparency, data integrity, process automation, and a high level of privacy. However, the question of data security arises considering the sensitivity of information in e-government. This paper explores the potential benefits of using blockchain technology in e-government while also emphasizing the need to research security aspects to ensure data reliability and protection. Through literature analysis and identification of key challenges, this paper highlights the significance of security in the application of blockchain technology in e-government and suggests directions for further research and development.

Keywords: e-government, blockchain, security

1. INTRODUCTION

Using technology is being used to simplify every aspect of life. The aim of every organization is to expedite basic processes and make them more accessible to users. E-government is a concept that plays a crucial role in the modernization and automation of public services. By utilizing information and communication technologies, the public sector aims to make its services more accessible to all citizens and thereby improve living conditions.

The public sector relies heavily on a large number of paper documents. Every interaction with the administration requires collecting a large number of papers from various institutions. This process often takes a lot of time. E-government represents a significant improvement because the goal is to digitize all documents. This significantly simplifies processes and saves time (Singh, 2023).

* *Corresponding author: marko.staka@uns.ac.rs*
Marko Štaka, ORCID: 0009-0004-5557-9096
Miroslav Stefanović, ORCID: 0000-0002-0767-365X
Darko Stefanović, ORCID: 0000-0001-9200-5092
Đorđe Pržulj, ORCID: 0000-0001-5951-563X
Vladimir Fabri, ORCID: 0000-0002-6218-7240

One of the key challenges that government institutions face is the distrust of citizens towards e-government. This distrust becomes a barrier to fulfilling the basic functions of public administrations and governments. The goal of every public administration and government is to build trust among citizens and demonstrate their capability and authority through an efficient and transparent system. However, when citizens lose trust in e-government due to fear of their data being misused, it negatively impacts the perception of government institutions. Data in e-government systems can often be exposed to third parties, whose access can result in alteration and misuse of the data. Lack of trust can lead to reduced collaboration between citizens and institutions, resulting in poorer service delivery efficiency and reduced legitimacy of government programs and policies. Therefore, it is important for government institutions to actively work on building trust through stringent security measures, transparency in data processing procedures, and educating citizens about their rights and the security measures in place.

Blockchain, as a distributed ledger of technology, offers a range of potential benefits for e-government (Lykidis et al., 2021). These benefits include decentralization, transparency, data integrity, process automation, and a high level of privacy. However, considering the sensitivity of the data processed within e-government, the question of data security and protection arises. The security aspects of blockchain technology require deeper research to ensure the reliability and protection of data from attacks, misuse, or unauthorized access.

Therefore, in this research, we explore the application of blockchain technology in e-government, highlighting the potential benefits of this technology, while also emphasizing the need to research security aspects to ensure safe and reliable use of blockchain technology in e-government. The application of blockchain technology in e-government is still a relatively new concept. Consequently, security shortcomings in the implementation of blockchain technology in e-government are mostly observed based on past applications and by analyzing the general security shortcomings of blockchain technology. In this section, a review has been conducted of previous papers that analyzed the application of blockchain technology in e-government services.

The paper presents examples of e-government in various countries based on blockchain technology. The paper is organized into 5 sections. Following this introductory paragraph, related works dealing with the application of blockchain in e-government are presented. The concept of e-government is outlined in the third paragraph. The fourth paragraph explains blockchain technology, its application in e-government, and identifies previous security shortcomings. The conclusion is presented in the fifth section, followed by a list of referenced works.

2. RELATED WORKS

A systemic review of software architecture types of blockchain-based applications in public administrations was conducted in (Lykidis et al., 2021). The result of this paper is the identification of e-government services that can benefit from the use of blockchain and the types of different technologies that would be used in these solutions. The aim of the work is to demonstrate the potential contribution of blockchain in this area.

In (Elisa et al., 2023) addresses the advantages and benefits brought by the implementation of blockchain in e-government. The theoretical analysis in this paper indicates that cryptography, immutability, and decentralized management and control offered by blockchain technologies can provide a certain level of security and privacy in e-government systems. The question arises whether that level is sufficient for mass adoption of e-government services. Security challenges regarding the application of blockchain in e-government are presented in (Elisa et al., 2023). This paper identifies the most common attacks on devices and proposes a new model based on artificial intelligence to reduce the likelihood of these attacks.

In Kadhum & Hamad (2023) it is conclude, through the analysis of two scenarios, that the performance of a blockchain network is influenced by hardware and software configurations, the complexity of smart contracts, and the scale of the organization.

The concept of applying blockchain technology in e-government is still primarily analyzed within a theoretical framework. Practical implementation may influence further research to fully understand the potential of blockchain technology in this area.

3. E- GOVERNMENT

The concept that involves the use of information and communication technologies for providing public services, managing processes, and facilitating communication between government institutions and citizens and the business sector is referred to as e-government. The goal of this concept is to digitize and automate traditional administrative processes to increase the availability of government services (Vereinte Nationen, 2022). Such digitalization enables the acceleration of administrative processes, faster processing of requests, reduction of administrative procedures, resulting in a decrease in the time required to obtain various documents and permits. There are four different types of interactions within e-government (Rachmawati et al., 2022):

- **G2C (Government-to-Citizen),** a term referring to communication between public administration and citizens. Services are usually provided through electronic channels. Examples of such services include online application for personal documents, tax filings, and permits.
- **G2G (Government-to-Government),** a term indicating communication between different sectors of public administration. It can involve communication between sectors at the same level or at different levels. An example is the exchange of information between ministries and local authorities.
- **G2B (Government-to-Business),** a term indicating communication between different sectors of public administration. It can involve communication between sectors at the same level or at different levels. An example is the exchange of information between ministries and local authorities.
- **G2E (Government-to-Employee),** a term indicating communication between the public sector and the employees comprising that sector.

The scheme of e-government types is depicted in Figure 1.

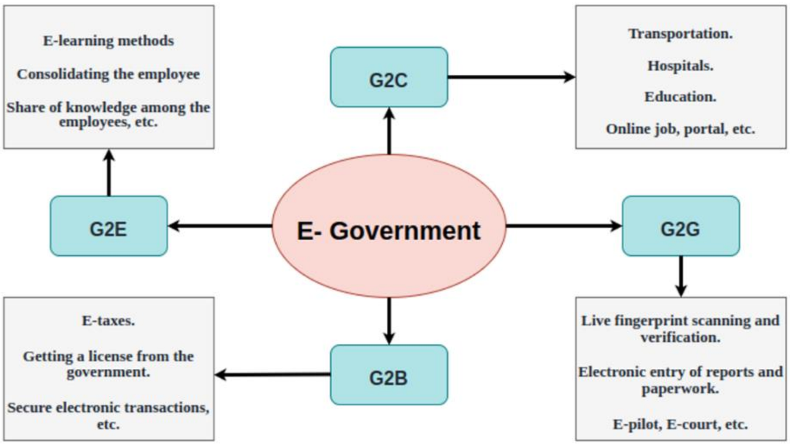
E-learning methods
Consolidating the employee
Share of knowledge among the employees, etc.
G2C
Transportation.
Hospitals.
Education.
Online job, portal, etc.
G2E
E- Government
G2G
E-taxes.
Getting a license from the government.
Secure electronic transactions, etc.
G2B
Live fingerprint scanning and verification.
Electronic entry of reports and paperwork.
E-pilot, E-court, etc.

Figure 1. Types of e-government (Elameer, 2021)

The monitoring of the development and implementation of e-government on a global level is supported by the United Nations. When discussing e-government development, the levels of G2C and G2B interactions are typically observed. The United Nations report for the year 2022 indicates that e-government is to some extent present in every country worldwide (Vereinte Nationen, 2022). The e-government development index (EDGI) is a measure of the level of e-government development in a country and is represented by a value between 0 and 1. According to the 2022 report, 60 UN member countries have an EDGI value in the range of 0.75 to 1. Compared to 2020, there has been an increase of 5.3% in this group, as there were 57 countries within this range at that time. 73 UN member countries have e-government developed in the range of 0.5 to 0.75, 53 countries in the range of 0.25 to 0.5, and only 7 countries have an EDGI value lower than 0.25. However, it is noted that no country has a value of 0, indicating that the e-government system is implemented to some extent worldwide.

The increased scope of e-government results in increased complexity and sensitivity of the system. The e-government system is one that needs to be distributed over typically large geographical areas and ensure data privacy. As a large number of different processes with a multitude of government, citizen, and business data are automated, maintaining the privacy and security of such transactions is challenging. Therefore, stricter measures and detailed analyses are required to prevent potential issues.

Every e-government system must guarantee confidentiality, integrity, and availability of services (Singh, 2023). Confidentiality implies that data within the e-government are not accessible to unauthorized persons. Integrity refers to ensuring that data within e-government are not modified or deleted by unauthorized users. The biggest challenge in maintaining most existing e-government systems is that websites and electronic identity management systems are centralized on duplicated servers and databases (Vereinte Nationen, 2022). The centralization of the system makes it vulnerable in terms of security and privacy because there is a "single point of failure." Such systems are targets of attacks such as DDoS (Distributed Denial of Service), DOS (Denial of Service), and malware. DOS attacks are a type of cyber attack aimed at disabling or limiting access to services, systems, or networks by flooding the target system or network with a large number of requests or traffic. The main goal of DOS attacks is to make services unavailable to legitimate users by preventing them from accessing the system or network. Therefore, the top priority of any government must be to ensure the highest level of privacy and security when using e-government services.

4. BLOCKCHAIN TECHNOLOGY

Blockchain is a relativity new technology. The beginning of blockchain technology is marked by the event of the publication of the paper 'Bitcoin: A Peer-to-Peer Electronic Cash System' in 2008. This paper was published by an individual or individuals using the pseudonym Satoshi Nakamoto. Blockchain is also referred to as a distributed ledger (Ibrahimy et al., 2024). The original purpose of blockchain technology was the exchange of digital currencies. The benefits of this technology have led to the recognition of its potential applications in other areas. Today, blockchain is used in the Internet of Things (IoT) (Huh et al., 2017), smart home development (Dorri et al., 2017), smart cities (Theodorou & Sklavos, 2019), the education system (Turkanovic et al., 2018), and healthcare (Peterson et al., 2016).

4.1. Application of blockchain technology in e-government

Blockchain technology emerges as a potentially safer solution in the development of e-government compared to previously created centralized systems. Blockchain technology achieves a decentralized environment for information exchange (Mukhopadhyay et al., 2016). The functioning of blockchain is recognized as a technology capable of providing a transparent and secure platform resistant to unauthorized storage and sharing of information. The idea is to utilize smart contracts for automating the delivery of government services, ensuring they are delivered in a secure and transparent manner, which is crucial for public administration (Kadhum & Hamad, 2023).

Smart contracts are programmable scripts that execute automatically when predefined conditions are met. They are a fundamental component of blockchain platforms like Ethereum. Smart contracts enable the automation and execution of various types of transactions or agreements without the need for intermediaries or centralized authorities. Smart contracts provide additional support for the development of e-government by allowing users to establish mutual agreements without the involvement of third-party intermediaries. These contracts are recorded on a public ledger. The application of smart contracts in establishing various agreements increases transaction speed.

The implementation of blockchain by governments and public institutions began by recognizing blockchain as a technology that would serve to replace previously implemented technologies, making processes more optimized. Alongside e-government, public institutions have started implementing blockchain in modern smart cities (Theodorou & Sklavos, 2019). In this paper, it is noted that this has led to improvements in the security of public data, as they are now being stored in various locations in block form. Each location contains an authentic copy of the stored information, and the absence of a third party reduces resource consumption.

In (Elisa et al., 2023) records the countries where e-government platforms based on blockchain were first implemented. The table is shown below.

Table 1. The list of countries with e-government projects based on blockchain technology is as follows

Country	Project description	Year of launch
Estonia	Implemented blockchain technology in electronic identification, e-health and e-residency.	2014.
UAE	Dubai initiated the implementation of a blockchain-based platform for the Department of Land. Since 2020, all public transactions have been conducted using blockchain technology.	2016.
China	Add blockchain integration to e-health, e-ID and e-voting systems.	2016.
France	Support the development of blockchain systems by banks and other business to enable secure business transactions.	2016.
Mexico	Embrace blockchain technology in finance, agriculture and public procurement.	2017.
Russia	Investigate the use of blockchain to manage government records, e-health services and land and property register.	2017.
Singapore	Since 2019, educational institutions have used the Ethereum blockchain to provide digital certificates.	2017.
Canada	Implemented blockchain technology in electronic identification, e-health and e-residency.	2018.
New Zealand	In 2018, blockchain was used in electronic voting.	2018.
Switzerland	The city of Zug launched an e-residency platform based on Ethereum.	2019.
Luxembourg	Create a public framework that will enable blockchain applications to be integrated into all industries.	2019.

Blockchain is now being applied in various e-government systems worldwide. One of the early examples is the launch of a platform by the Dubai Land Department (Theodorou & Sklavos, 2019). The platform allows citizens to register all property documents, such as ownership deeds, sale contracts, and inheritance contracts, without the need to physically visit a building or office. This has significantly expedited the process of obtaining such documents and shortened the time for property transactions. The platforms started operating in 2016, and by 2020, all public transactions were conducted using blockchain.

Another example of blockchain implementation in e-government is registered in Estonia (*Become an E-Resident of Estonia, How to Apply*, 2024). Estonia introduced the concept of e-residency as early as 2014, which served as a precursor to today's e-government system in the country. Today, the system is called e-Estonia (*E-Estonia*, 2024) and features various blockchain-based platforms that allow citizens to establish companies online, conduct business banking, electronically sign documents, and electronically submit tax and other business filings.

4.2. Security vulnerabilities

It has been determined that more than 80% of websites worldwide were vulnerable to Cross-Site Scripting (XSS) and Structured Query Language (SQL) Injection attacks due to the lack of appropriate authentication mechanisms applied to user input (Moen et al., 2007). Due to the nature of the data within e-government frameworks, this system often faces various security issues. Data loss within e-government can have significant economic, legal, and social consequences. Social consequences manifest in decreased support and trust from e-government users. The e-government support issue is precisely the lack of confidence among citizens who are unsure whether they can leave their private data on various websites. Past negative experiences have a detrimental impact on citizen trust. In 2014, Singapore experienced an attack on over 1,500 user accounts (*The Role of Central Signing and Authentication in E-Government Security*, 2024). Following the attack, hackers gained access to opening new businesses and applying for work permits. One of the biggest hacks on the e-government system was in 2015 in the United States when over 4 million government employee records were leaked (*The Role of Central Signing and Authentication in E-Government Security*, 2024). The leaked data included security clearance information, social security numbers, identities, and passwords of official accounts. A year later, in 2016, cyber terrorists attacked the Tanzanian government, causing around $85 million in damages (Elisa et al., 2023).

The main reason for the adoption of blockchain technology is achieving a higher level of interoperability. Therefore, the application of blockchain in these applications can alleviate some of the drawbacks of other technologies. However, the implementation of blockchain can also bring about new challenges. A potential issue arises when multiple system components are built using different technologies. Different generations of blockchain are vulnerable to different attacks.

Security risks in blockchain applications in e-government are usually divided into two main categories. The first category includes risks that can affect both Blockchain 1.0 and Blockchain 2.0/3.0, while the second group consists only of those affecting Blockchain 2.0/3.0.

The Majority Attack or 51% Attacks are described in (Mansour et al., 2023) as a flaw in blockchain that can have negative effects on its implementation in systems such as e-government. It is one of the most commonly mentioned risks of blockchain-based applications. The attack is executed if one organization or a coalition of other organizations enhances mining capability using the proof of work algorithm (POW). When 51% control of the total chain's power is achieved, the organization has the ability to invalidate transactions or decide which block will be allowed to execute. In such a case, the entity has the ability to create the longest chain of blocks. The chain created by that entity can be accepted by the entire network without being validated, representing a security risk (Singh et al., 2021). This flaw should be especially considered regarding implementation in e-government, given that e-government systems must be protected from malicious attacks that could cause interruptions or data leaks.

The self-mining approach to mining is a risk that belongs to the first category of security risks. It represents a malicious occurrence where a malicious entity is provided with more tokens than it rightfully owns. The entity is called a pool and represents a group of miners who combine their computational resources to collectively work on finding new blocks and securing transactions on the blockchain. This can lead to certain entities having control over the network, even though their share is less than 51%. In this case, the malicious entity has the ability to reap all the benefits of transactions. This will make the network unprofitable for other nodes, which may decide to leave. In such a scenario, the malicious pool can facilitate double spending and prevent the execution of transactions they do not wish to be executed (Sapirshtein et al., 2017).

Eclipse attacks occur when an attacker gains control over the connections of the victim node, taking control of both outbound and inbound connections. This effectively blinds the victim node, leading to unnecessary resource consumption. Subsequently, the attacker has an easier time executing a 51% attack or other malicious activities (Heilman et al., n.d.).

DDoS attacks are not specific to blockchain applications alone. The attacker's objective is to take control of the network by overwhelming it with a large number of requests. In (Vasek et al., 2014), it was shown that about 25% of observed pools between 2011 and 2013 were subjected to DDoS attacks.

The second group of risks to Blockchain 2.0/3.0 consists of risks associated with smart contracts. As highlighted earlier, a significant number of applications in e-government today are based on smart contracts, making it crucial to analyze these vulnerabilities. In Wang et al. (2018), it is highlights the vulnerability of systems built on the principle of smart contracts. When a contract invokes multiple transactions, the order of their execution affects the new state of the chain. A re-entrant call to the contract can pose a security flaw, as in this case, an attacker can exploit the intermediate state and cause unexpected behavior, currency theft, or influence increased spending. This undesired outcome is referred to as Transaction-Ordering Dependence. Such a security breach can impair various functionalities of e-government.

Executing a smart contract requires paying a fee. The fee price depends on the contract structure and the gas price at the time of execution. Poorly structured smart contracts affect the increase in the contract execution price. A negative impact on gas price has a dead code. Dead code is part of the code that exists but will never be executed. Such code affects the increase in the cost of executing a smart contract. Poorly structured code that consumes more gas during execution makes it easier for attackers to launch a DDoS attack on Ethereum.

In Atzei et al. (2017), a taxonomy of smart contract vulnerabilities is highlighted. Within it, vulnerabilities are classified based on levels and causes. At the level of the Solidity programming language, which is characteristic for writing smart contracts, vulnerabilities such as Call to unknown, Gasless send, Reentrancy, and Keeping secrets are mentioned.

The first vulnerability mentioned, Call to unknown, refers to the situation when the *fallback()* method is invoked in the Solidity programming language. When this call does not correspond to any existing function, it allows an attacker to invoke certain built-in functions that enable the transfer of Ether to another address. Examples of functions that an attacker can call include *call(), send(),* or *delegateCall().*

When creating a smart contract, care should be taken to ensure gas forwarding to avoid the occurrence of Gasless send. If a sufficient amount of gas is not forwarded to the smart contract function during invocation, the transaction will be reverted, and gas will be charged (Macrinici et al., 2018).

The previously mentioned *fallback()* mechanism can disrupt the rule that a non-reentrant function should be called before its completion. This can lead to the occurrence of reentrancy, where the function execution happens continuously until all gas is consumed.

Keeping secrets cause represents a case when we want a variable in the smart contract to be private. Such fields should be hidden. Setting the value of a private field requires sending a transaction to the smart contract, and transactions in the blockchain are public elements, so it is possible to see the values of private fields from them. Therefore, the solution for keeping values private involves the application of cryptographic techniques.

In addition to blockchain characteristics, legal and regulatory barriers can also have a negative impact on security. State legal regulations may influence the faster implementation of blockchain-based services in some areas compared to others. This affects the slowdown in the broader implementation of blockchain applications for e-government.

The e-government system encompasses a vast amount of important data. Besides the internal security issues mentioned, there arises a question of the credibility of this data upon entry into the system. One of the issues regarding smart contract technology is the inability to interact with resources outside the network of nodes on which the smart contracts are executed. If smart contracts were implemented to rely solely on a centralized data source, the essence of decentralization would lose its advantages. Chainlink presents a solution to this problem. Chainlink utilizes various nodes to obtain the requested data. They provide consensus and establish consensus before returning the data to the smart contract. This way, the smart contract does not rely solely on one source.

Blockchain drawbacks can particularly manifest when the technology is applied for various purposes. The basic idea presented in Elisa et al. (2023) and Mansour et al. (2023) is to structure a combination of such models that, in addition to blockchain, will also use other technologies, such as artificial intelligence, to protect the system from potential attacks. Governance model, storage criteria, and access control are fundamental elements with potential vulnerabilities that need attention. Conducting empirical studies can reveal a greater number of drawbacks and issues to consider when developing a component of a serious system like the e-government system.

5. CONCLUSION

Blockchain technology has been identified as a significant tool in building complex systems with a large number of participants and important tasks, such as e-government systems. Based on previous research and various systems worldwide, it has been concluded that blockchain-based e-government can provide a higher level of security and integrity. Such a system remains decentralized and more transparent while maintaining data integrity.

However, considering that blockchain is a relatively new technology, its implementation should be carefully considered and addressed whenever used in building components of e-government systems. Despite being the best solution today, its application presents certain security challenges.

This paper provided an overview of the application of blockchain technology in e-government systems worldwide and emphasized their significance. Subsequently, the basic drawbacks of blockchain technology that have negative effects on e-government operations were summarized. It was observed that in certain cases, the system becomes more susceptible to attacks, which should not be tolerated in e-government development. Additionally, certain use cases of e-government pose security challenges regarding privacy, performance, and scalability.

Addressing these challenges requires thorough research, the development of advanced security mechanisms, and collaboration among information security experts, legal professionals, and government agencies to ensure the secure and efficient use of blockchain technology in e-government.

ACKNOWLEDGMENT

This research (paper) has been supported by the Ministry of Science, Technological Development and Innovation through project no. 451-03-47/2023-01/200156 “Innovative scientific and artistic research from the FTS (activity) domain”.

REFERENCES

Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A Survey of Attacks on Ethereum Smart Contracts (SoK). In M. Maffei & M. Ryan (Eds.), *Principles of Security and Trust*, Vol. 10204, 164–186. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-54455-6_8

Become an e-resident of Estonia, how to apply. (2024, April 7). E-Residency. https://www.e-resident.gov.ee/become-an-e-resident/

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 618–623. https://doi.org/10.1109/PERCOMW.2017.7917634

E-estonia. (2024, April 7). Estonia.Ee. https://estonia.ee/enter/

Elameer, A. (2021). COVID-19 and real e-government and e-learning Adoption in Iraq. https://doi.org/10.1109/IICETA51758.2021.9717570

Elisa, N., Yang, L., Chao, F., & Cao, Y. (2023). A framework of blockchain-based secure and privacy-preserving E-government system. *Wireless Networks*, *29*(3), 1005–1015. https://doi.org/10.1007/s11276-018-1883-0

Elisa, N., Yang, L., Chao, F., Naik, N., & Boongoen, T. (2023). A Secure and Privacy-Preserving E-Government Framework Using Blockchain and Artificial Immunity. *IEEE Access*, *11*, 8773–8789. https://doi.org/10.1109/ACCESS.2023.3239814

Heilman, E., Kendler, A., Zohar, A., & Goldberg, S. (n.d.). Eclipse Attacks on Bitcoin’s Peer-to-Peer Network.

Huh, S., Cho, S., & Kim, S. (2017). Managing IoT Devices using Blockchain Platform.

Ibrahimy, M. M., Norta, A., & Normak, P. (2024). Blockchain-based governance models supporting corruption-transparency: A systematic literature review. *Blockchain: Research and Applications*, *5*(2), 100186. https://doi.org/10.1016/j.bcra.2023.100186

Kadhum, O. I., & Hamad, A. H. (2023). Performance Evaluation of Multi-Organization E-Government Based on Hyperledger Fabric Blockchain Platform. *Ingénierie Des Systèmes d Information*, *28*(2), 499–507. https://doi.org/10.18280/isi.280227

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

Macrinici, D., Cartofeanu, C., & Gao, S. (2018). Smart contract applications within blockchain technology: A systematic mapping study. *Telematics and Informatics*, *35*(8), 2337–2354. https://doi.org/10.1016/j.tele.2018.10.004

Mansour, M., Salama, M., Helmi, H., & Mursi, M. F. M. (2023). A Survey on Blockchain in E-Government Services: Status and Challenges. *International Journal of Engineering Research*, *12*(04).

Moen, V., Klingsheim, A. N., Simonsen, K. I. F., & Hole, K. J. (2007). Vulnerabilities in e-governments. *International Journal of Electronic Security and Digital Forensics*, *1*(1), 89. https://doi.org/10.1504/IJESDF.2007.013595

Mukhopadhyay, U., Skjellum, A., Hambolu, O., Oakley, J., Yu, L., & Brooks, R. (2016). A brief survey of Cryptocurrency systems. 2016 14th Annual Conference on Privacy, Security and Trust *(PST)*, 745–752. https://doi.org/10.1109/PST.2016.7906988

Peterson, K., Deeduvanu, R., Kanjamala, P., & Boles, K. (2016). A Blockchain-Based Approach to Health Information Exchange Networks.

Rachmawati, Aswar, K., Sumardjo, M., Wiguna, M., & Hariyani, E. (2022). Personal and reliability factors affecting adoption and utilization of e-government: An effect of intention to use. *Problems and Perspectives in Management*, *20*(2), 281–290. https://doi.org/10.21511/ppm.20(2).2022.23

Sapirshtein, A., Sompolinsky, Y., & Zohar, A. (2017). Optimal Selfish Mining Strategies in Bitcoin. In J. Grossklags & B. Preneel (Eds.), *Financial Cryptography and Data Security*, Vol. 9603, 515–532. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-54970-4_30

Singh, D. A. (2023). *E-GOVERNANCE: MOVING TOWARDS DIGITAL GOVERNANCE*. *2*(1).

Singh, S., Hosen, A. S. M. S., & Yoon, B. (2021). Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network. *IEEE Access*, *9*, 13938–13959. https://doi.org/10.1109/ACCESS.2021.3051602

The Role of Central Signing and Authentication in e-Government Security. (2024, April 7). https://www.cryptomathic.com/news-events/blog/key-for-egovernment-security-central-signing-authentication

Theodorou, S., & Sklavos, N. (2019). Blockchain-Based Security and Privacy in Smart Cities. In *Smart Cities Cybersecurity and Privacy* (pp. 21–37). Elsevier. https://doi.org/10.1016/B978-0-12-815032-0.00003-2

Turkanovic, M., Holbl, M., Kosic, K., Hericko, M., & Kamisalic, A. (2018). EduCTX: A Blockchain-Based Higher Education Credit Platform. *IEEE Access*, *6*, 5112–5127. https://doi.org/10.1109/ACCESS.2018.2789929

Vasek, M., Thornton, M., & Moore, T. (2014). Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem. In R. Böhme, M. Brenner, T. Moore, & M. Smith (Eds.), *Financial Cryptography and Data Security* (Vol. 8438, pp. 57–71). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-44774-1_5

Vereinte Nationen (Ed.). (2022). The future of digital government. United Nations.

Wang, S., Yuan, Y., Wang, X., Li, J., Qin, R., & Wang, F.-Y. (2018). An Overview of Smart Contract: Architecture, Applications, and Future Trends. 2018 IEEE Intelligent Vehicles Symposium (IV), 108–113. https://doi.org/10.1109/IVS.2018.8500488