Analysis of Cyber Security In E-Governance Utilizing Blockchain Performance

Regonda Nagaraju (regondaphd2021@yahoo.com)
St.Martin's engineering College
Selvanayaki Kolandapalayam Shanmugam
Ashland University
Sivaram Rajeyyagari
Shaqra University
Jupeth Toriano Pentang
Western Philippines University
B Kiran Bala
K Ramakrishnan College of Engineering
Arjun Subburaj
Sentinel Management Group Inc
M.Z.M. Nomani
Aligarh Muslim University

Research Article

Keywords: Decentralized systems, block chain technology, e-government, privacy, security etc.

Posted Date: September 30th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-938929/v1

Abstract

E-Government refers to the administration of Information and Communication Technologies (ICT) to the procedures and functions of the government with the objective of enhancing the transparency, efficiency and participation of the citizens. E-Government is tough systems that require distribution, protection of privacy and security and collapse of these could result in social and economic costs on a large scale. Many of the available e-government systems like electronic identity system of management (eIDs), websites are established at duplicated databases and servers. An established validation and management system could face a single failure point and the system is prone to Distributed Denial of Service Attacks (DDoS), denial of service attacks (DoS), malware and other cyber attacks. The execution of a privacy preserving and a secure decentralized system is enabled by the block chain technology. Here any third-party organizations do not have any control over the transactions of the Government. With the help of block chain technology, new and existing data are encapsulated within ledger or blocks, which are evenly distributed through the network in an enduring and sustainable way. The privacy and security of information are improved with the help of block chain technology, where distribution and encryption of data are performed through the total network. This analytical paper maps out the analysis of the security in the e-government system, utilizing the block chain technology that provides privacy and security of information and thereby enhancing the trust among the public sector. Qualitative and theoretical analysis is made for the proposed topic and implications of privacy and security of the proposed system is made.

I. Introduction

The internet around the world motivates various countries of the world for exploiting technologies as forms of services and communication exchange between affiliates and citizens. The users of e-Government make use of the services online, without stepping out their homes, minimizing the long queues at the offices of the public sector, thereby saving transportation costs and time with an alternate delivery of services with efficiency and effectiveness (). Government networks have an efficient form of communication, when compared with the business networks (Elisa et.al 2018). It is due to their information transfer and exchange to the public in the absence of competition. There would be a dramatically increase of e-government services by many devices in the future, because of the rigid progression of interconnected networks, smart cities, internet of things (IOT), smart homes etc. Based on an e-government survey of the United Nations, which was conducted in the year 2014, most of the government services of the countries around the world provide their stakeholders and citizens with e-services through mobile applications and websites. The e-Government systems involve collection, storage and information processing regarding financial status, researches, products, services, customers, employees, citizens and others utilizing the electronic devices. This information might be confidential and may result in loss of financial advantages, opportunities, confidence and trust of the users. Results of several services reveals that about 80% of the websites related to e-government around the world are susceptible to structured query injection (SQL) and cross-site scripting (XSS), because of the absence of appropriate mechanism of authentication endeavored to the users’ input data. Malwares, denial of service attacks etc., affects the information exchange in many countries in the world. These are threats or barriers in providing services online. The threats related to security are present in the developed countries as well (Shareef M. Shareef 2017). For instance; a loss of about $85 million were made by the digital fraudsters, hackers, technology spies and cyber terrorists to the Tanzania Government in the year 2016. In Singapore, about 1500 accounts of various users were hacked by the hackers, which were stored in the e-Government platforms in the year 2014. There are many other archetypes for the e-Government threats.

Thus, it is essential to protect and preserve the availability, integrity, confidentiality, privacy and security of the e-government systems. There is a chance for the security and privacy breaches of an e-government system, when proper counter measures and security techniques are not constructed and are made ready for overcoming these internet threats in the future. The block chain technology becomes one among the solutions for offering a secure and private environment for exchange of confidential information. Earlier, the block chain technology was developed for the exchange of digital currency. Then this technology is endeavored in healthcare, educational systems, smart city, smart home and internet of things (IOT). Many countries do not make use of the block chain technology in their public operations and services, but have started using it for exploring the block chain technology potential for providing the individuals with public services. These services may be land registry, e-health, e-residency etc. This analytical paper provides an analysis about how the block chain technology helps in protecting and securing the e-Government information. This paper encapsulates a block chain framework whose performance confirms the protection of e-Government information with the help of block chain technology. The initial portion of the paper is dealt with the theoretical background of the study, then about the existing literature of the proposed study, then about the e-government system based on block chain, then the privacy and security analysis of the block chain performance utilized in e-Government security and the final portion of the paper is dealt with the complexities and challenges in endeavouring the block chain technology to the systems of e-Government.

Ii. Theoretical Background

This section provides a brief note on the e-Government systems and the block chain technology.

a. E-Government Systems

E-Government refers to the provision of Government services and information online through any digital means or the internet (M. Alsheri and S. Drew 2010). E-Government delivers government services and information to the government agencies, business and citizens. There are three eminent classifications of the services provided by e-Government. They are; government to business (G2B) service, government to citizen service (G2C) and government to government service (G2G). The government-to-government service provides interaction online between organizations, authorities and departments of the government to exchange information between them with the utilization of the internet. Government to business (G2B) and government to citizens (G2C) services allow businesses and citizens to have government interactions for getting online services like, e-procurement application, online voting, licenses and passport, renewal/

extending of visa, filling of income tax, property tax etc. Only authorized users could access the confidential information of individuals, which is confirmed by each department in the e-government building of a reliable system that is relied by the users, is an essential factor to be considered during the implementation of e-government. In an e-government system, assurance of privacy and security acts as a critical factor to increase the reliability between various departments of the government. This in turn helps in getting privileged access to confidential information and gain integrity. Phishing, DDoS, malware, probes etc. are some cyber attacks, which are faced by the e-government systems. It is because of these cyber attacks, there are possibilities for supremacy contests, cyber terrorism, extortion, political differences etc., which happens between various nations or occurs within one nation. The privacy and security of e-government systems are offered utilizing anti-virus mechanisms, Public Key Infrastructure (PKI), Intrusion Detection Systems (IDS) and firewalls. e-ID system is utilized to deal with the security issues of e-government systems such as for integrity, confidentiality, authentication and for identification of information of the users.

b. Block chain technology

Block chain technology refers to a structure, which encapsulates many records of transactions called the public block, which is stored in various databases that are connected across a network with peer-to-peer nodes. This structure is otherwise called a digital ledger (simple learn 2021). A block chain functions in the form of immutable ledger that enables transactions to happen in a decentralized form. The block chain based endeavors are rising at present that has internet of things (IoT), reputation systems, financial services etc. But it has some security and scalability issues, which has to be resolved (Zheng et.al 2017). Some of the block chain benefits comprise of openness, tamper-proof construction, transparency of information, decentralization and distributed ledger. Depending upon their application, the block chains are classified as 3.0, 2.0 and 1.0. Block chain technology is also endeavored in copyright protection, smart energy, market analysis, supply chain management, government functions and healthcare (Xu et.al 2019). The following figure indicates a typical block chain architecture that comprise of a series of blocks of data.

Block chain architecture

The block chain architecture comprise of a series of block sequence that encapsulates a total list of transactions; Example; a public ledger. In the block chain architecture, the large block is the block header, which has six other blocks such as parent block hash, nonce, n Bits, time stamp, merkle tree root hash and block version. Within the block header, only one block would be a parent block. In the block chain architecture, the initial block is known as the genesis block, which lacks any parent block. The block chain architecture comprise of blocks and digital signature. A block comprise of a block body and block header as represented in the below figure.

The block header comprise of block version that represents the rules of block validation that is to be followed. In a block, the entire transactions' hash value is represented in the Merkle tree root hash. The present universal time in seconds is represented in the time stamp. A valid block's hash value is indicated as the target threshold in the n-bits. Nonce indicates a 4 byte field that initiates from zero and rises for each calculation of hash. The parent block indicates the 256 bit hash value, which represents the block of the previous section. Transactions and transaction counter are encapsulated within the block body. An asymmetric cryptographic technique is utilized by the block chain for validating transactions' authentication. Digital signature is contemplated on the above technique. Pair of public and private keys is owned by every user. The transactions are signed by the confidential private key. Thus, verification and signing phases are included in the digital signature. In a block chain technology, the striking features are decentralization, persistency, anonymity and auditability.

Iii. Literature Review

(Zhao S. and Zhao J. 2010) conducted an analysis on the e-government systems, which were under the control of the United States for analyzing the threats and opportunities happening to the country's internet users. Most of the countries' sites indicated clearly the security measures of the U.S. government. SSL encryption was utilized by about 98% sites for protecting the accounts of the users. Web content analysis, security mapping in the computer networks and information security auditing methods were carried out in their analysis. Many security lapses were identified in their research and they failed in providing resolutions to those issues.

(Drew S. and Alsheri M. 2010) analyzed the barriers and challenges, which happened in the implementation of e-government transactions made by the Saudi citizens. Data analysis and online survey were the tools utilized by them for their analysis. The drawback of their research was that the security needs were not properly explored by them.

(Gabriel B. 2018) analyzed the confidence and trust level of the public in the security of systems and data, which are exchanged on the e-government platform of Ghana with the contemplation on integrity and data protection. The results of the study indicated that a high drawback is observed in the e-governance data integrity, continuous availability of services and confidentiality issues. The e-government services are focused in their study with a cross-sectional survey. It was carried out in four regions of Ghana. The drawback of his research was that solutions were not offered to poor internet, exclusion of service, verification of information in the national database etc.

(Haran M. 2016) analyzed the inside stakeholders of the e-government sector in the IT field and listed out the possible attacks, which are created by these people. Solutions were provided for resolving those threats. A robust mechanism or framework was proposed for mitigating and detecting these threats in an early manner. He insisted that those threats were surely caused by the inside stakeholders. Early exploration and resolution ways of those threats were highlighted as essential in his paper. The drawback of his analysis was that the insider threats were only analyzed in his research (murugesan S et al. 2013).

(Rajandran K. and Mohamed R. 2017) examined the reason for the less participation of the people in e-government transactions in Thanjavur, a district in India and concluded that the reasons for their less participation were; e-governance security, attitude for development with sustainability, acceptance and awareness level. Correlation analysis, regression and random sampling were the tools of research involved in their examination. The drawbacks of their research were that the sample size was small; improvement was needed in the web security of the e-government and those improvements were not mentioned in their paper (Manoj R et al. 2013).

Iv. E-government System Based On Block Chain

A framework for the block chain technology based on e-government systems is shown in the below figure.

In the above figure, the double arrow indicates the transactions happening between different nodes, which represent the organizations, authorities or departments of the government with the citizens and businesses. This forms a peer-to-peer network for exchanging and validating data, which are exchanged by different individuals. A government to citizen (G2C) arrow indicates the information that is exchanged between the government and the citizens such as passport or visa, birth certificates, business permits, marriage certificates, tax reports etc. The government to business arrow indicates the exchange of information between the businesses and the government. These include; electronic auctions, insurance clearance forms etc. Any new user node or e-government node requires e-government tokens and review of network peers to be added in the block chain network. In a block chain network, the total number of stored records will be equal to the total number of tokens of e-government. In a block chain network, there are two nodes, which are important such as light weight node and full nodes. In the system proposed here, the e-government nodes are the full nodes and the devices of the users are the light weight nodes, which are B and C nodes. In the system proposed here, the connectivity to the network is offered by the wireless broadband or Wi-Fi. There are separate algorithms for creation of a node in the e-government network. The e-government systems could construct a full network node and only light weight nodes could be set up by the users. Post the addition of a new node to the e-government network, the broadcast of the registration is carried to the peers of the network using delegate lines, which are assigned to the network peers. The process of information security is carried out utilizing the distributed and encrypted data within the network. An active is involved in the creation of each new block.

a. Privacy and Security Analysis

The services availability, integrity and confidentiality must be ensured by the e-government systems. When there is disclosure of information with the unauthorized users, there is achievement of confidentiality. Integrity is gained with the information protection, without any modification. The storage of records in the system presented here is done with the help of public key cryptography, which provides protection from any unauthorized access. Digital signature and encryption are utilized in the e-government systems for confirming access control, privacy and security to the records in the block chain e-government network. A record is altered with an attack happening the peer network. A block in the block chain network is modified with the modification made by the attacker and thus a new block is replaced there. The stored data privacy is increased in the presented network with the hashing of blocks of all the users. In the block chain there is storage of all the user transactions' hashes, which are incomprehensible.

b. Complexities and Challenges

The block chain technology's ability for recording the distributed ledger transactions provides newer chances for the government for enhancing transparency construct reliability in public transactions and protects against frauds. But the adoption of block chain technology and its utilization in the e-government systems is not explored yet. Many study results about the relationship between the block chain technology and the e-government systems indicates that the endeavoring of the block chain in the e-government systems is less available and empirical evidence is absent it. The complex challenges that happen in the adoption of the block chain technology in the e-government systems are flexibility, scalability and security (Batubara et.al 2018). On the organizational perception, the requirement of new models of governance and acceptability issues are found as important adoption barriers. Also the absence of regulatory and legal support is indicated as an eminent adoption challenge. With the above complexities and challenges, future research is essential in the adoption of block chain technology in the public sectors.

Iv. Conclusion

Thus, this presented analysis makes a conclusion that the block chain technology adoption in the public or e-government sector is a rising platform for innovation in the future, which covers almost all the sectors and also the public sector. The block chain technology acts as an infrastructure for support in the handling and protection of information and it provides an eminent effect on the digital innovations in the future, which also has the government sector. Thus, the block chain technology-based ICT systems indicate a decentralized control and management and provides flexible and robust resolutions, without corruption. Thus, an e-government framework of block chain technology that provides privacy and security in the government sector is proposed. The qualitative and theoretical analysis of privacy and security of the system proposed here indicates that, a decentralized control and management, immutability and cryptography enhance privacy and security in the systems of e-government. The interoperability issues of the government departments are also resolved with the presented system. Furthermore, research is essential to be implemented in the block chain technology adoption in the e-government sector.

Declarations

Ethical Compliance

Not applicable

Acknowledgments

All authors have seen the manuscript and approved to submit it to the journal.

Conflicts of Interest

Authors say there is no conflict of interest

Funding

There is no funding

Informed Consent

All authors have seen the manuscript and approved to submit it to the journal.

Author contributions

All authors have seen the manuscript and approved to submit it to the journal.

References

1. Elisa, Noe, et al. “A Framework of Blockchain-Based Secure and Privacy-Preserving E-Government System.” Wireless Networks, Dec. 2018. Springer Link, doi:10.1007/s11276-018-1883-0
2. Shareef M. Shareef. Security of E-Government; Risks, Threats, and Success Factors. no. 10, Mar. 2017, pp. 61–78
3. Geoffrey Rwezaura Karokola. A Framework for Securing E-Government Services. Stockholm University, 2012, https://www.diva-portal.org/smash/get/diva2:557279/FULLTEXT04.pdf
4. Alshehri, Mohammed, and Drew S. “Implementation of E-Government: Advantages and Challenges.” Undefined, 2010, https://www.semanticscholar.org/paper/Implementation-of-e-Government%3A-Advantages-and-Alshehri-Drew/de9d2e9f2bbf69e04e397f01f0ccd5689dbead76
5. Haitham Assiri P Nanda and Manoranjan Mohanty. Secure E-Governance Using Blockchain. Easy Chair, 23 Sept. 2020, https://easychair.org/publications/preprint_open/svXR
6. Gondek, Basic Blockchain Technology CA PPT Presentation That You Can Use. https://originstamp.com/blog/blockchain-technology-ppt-presentation/. Accessed 21 May 2021
7. Xu, Min, et al. “A Systematic Review of Blockchain.” Financial Innovation, vol. 5, no. 1, July 2019, p. 27. BioMed Central, doi:10.1186/s40854-019-0147-z
8. Leible, Stephan, et al. “A Review on Blockchain Technology and Blockchain Projects Fostering Open Science.” Frontiers in Blockchain, vol. 2, 2019. Frontiers, doi:10.3389/fbloc.2019.00016
9. Zheng, Zibin, et al. “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends.” 2017 IEEE International Congress on Big Data (BigData Congress), 2017, pp. 557–64. IEEE Xplore, doi:10.1109/BigDataCongress.2017.85

10. “What Is Blockchain Technology and Why Is It Popular.” Simplilearn.Com, https://www.simplilearn.com/tutorials/blockchain-tutorial/blockchain-technology. Accessed 21 May 2021
11. “Architecture of Blockchain.” Advances in Computers, vol. 121, Jan. 2021, pp. 171–92. www.sciencedirect.com, doi:10.1016/bs.adcom.2020.08.009
12. Batubara F, Rizal et al. “Challenges of Blockchain Technology Adoption for E-Government: A Systematic Literature Review.” Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age, Association for Computing Machinery, 2018, pp. 1–9. ACM Digital Library, doi:10.1145/3209281.3209317
13. Research (IJSR), International Journal of Science and. “International Journal of Science and Research (IJSR).” International Journal of Science and Research (IJSR). www.ijsr.net, https://www.ijsr.net/get_abstract.php?paper_id=20131337. Accessed 21 May 2021
14. Alshehri, Mohammed, and Steve Drew. “Challenges of E-Government Services Adoption in Saudi Arabia from an e-Ready Citizen.” Undefined, 2010, https://www.semanticscholar.org/paper/Challenges-of-e-Government-Services-Adoption-in-an-Alshehri-Drew/307d0682a3f91d4800040cb94935a7c4db48310b
15. Zhao, Jensen J et al. “Opportunities and Threats: A Security Assessment of State e-Government Websites.” Government Information Quarterly, vol. 1, no. 27, 2010, pp. 49–56. www.infona.pl, doi:10.1016/j.giq.2009.07.004
16. Gabriel Botchwey. “E-Governance and Cybersecurity: User Perceptions of Data Integrity and Protection in Ghana.” E-Governance and Cyber Security, 2018, pp. 1–22
17. Mohamed, R. and Rajandran KA Study on Cyber Security in E-Governance with Reference to Areas of Thanjavur District, Tamil Nadu. 2017
18. Manoj R, Dr. Senthil Kumar T, Maruthi M, Vivek G, “A Survey: Artificial Neural Networks in Surveillance System”, International Journal of Computer Applications,VOL.1,PP.19–22,2013
19. Murugesan S, Dr. Senthil Kumar T, Priyanka U, Sree, Abinaya K, “Towards an Approach for Improved Security in Wireless Networks”, International Journal of Computer Applications, vol. 1, pp. 9–13, 2013

Figures

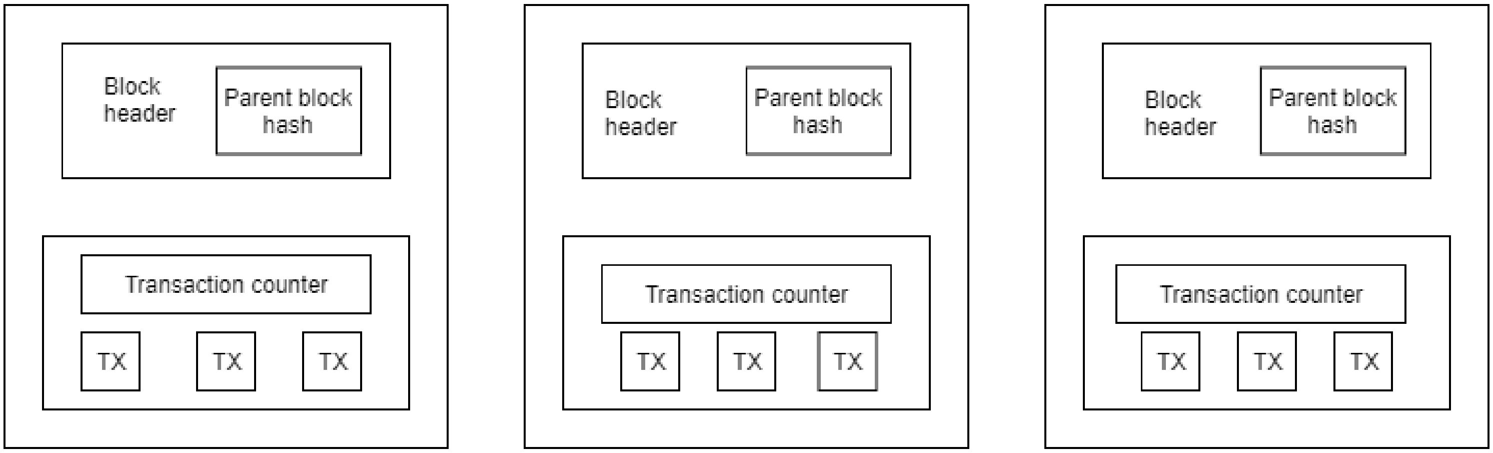

Figure 1

Block chain architecture

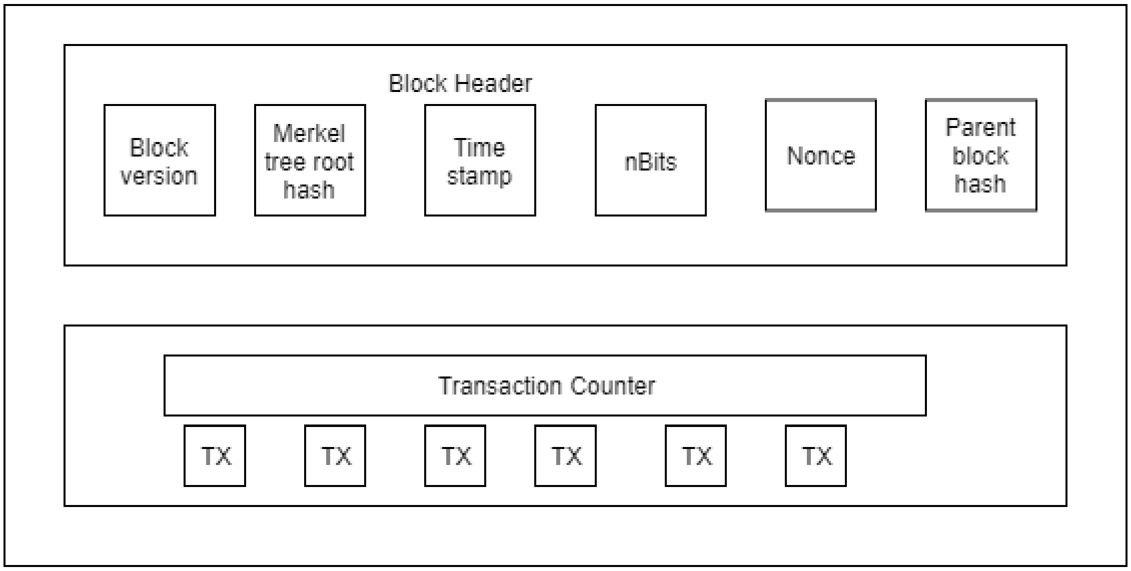

Figure 2

The block header comprise of block version that represents the rules of block validation that is to be followed. In a block, the entire transactions' hash value is represented in the Merkle tree root hash. The present universal time in seconds is represented in the time stamp. A valid block's hash value is indicated as the target threshold in the n-bits. Nonce indicates a 4 byte field that initiates from zero and rises for each calculation of hash. The parent block indicates the 256 bit hash value, which represents the block of the previous section. Transactions and transaction counter are encapsulated within the block body. An asymmetric cryptographic technique is utilized by the block chain for validating transactions' authentication. Digital signature is contemplated on the above technique. Pair of public and private keys is owned by every user. The transactions are signed by the confidential private key. Thus, verification and signing phases are included in the digital signature. In a block chain technology, the striking features are decentralization, persistency, anonymity and auditability.

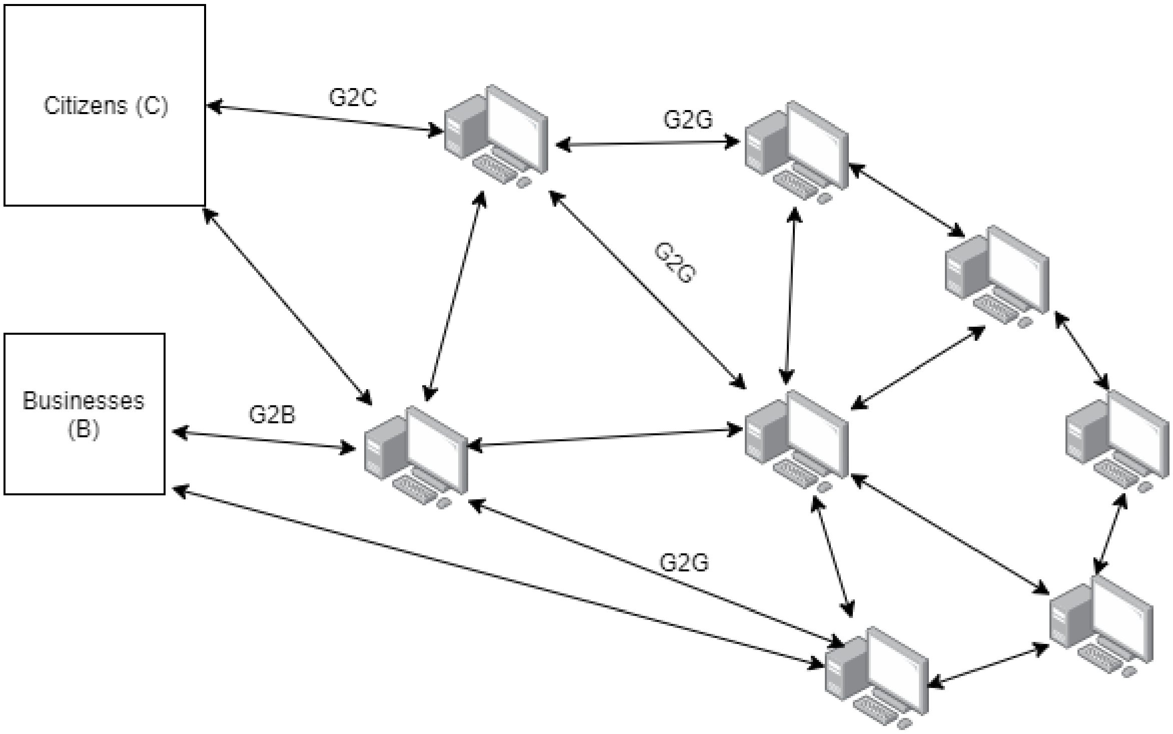

Figure 3

e-Government network based on block chain technology