iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VIII **Month of publication:** August 2022

DOI: https://doi.org/10.22214/ijraset.2022.46487

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VIII August 2022- Available at www.ijraset.com

Blockchain Technology for e-Government

Rajesh B. Walde[1], Amit Kumar Yadav[2]
[1, 2]*G B Pant DSEU Okhla-III Campus, New Delhi*

Abstract: ***Information and communication technologies are used by e-Government to deliver governmental services to people and companies instantly, effectively, and efficiently. The majority of current e-government systems are centrally located on redundant servers and databases that may have single points of failure, rendering the systems susceptible to cyber-attacks. Blockchain technology makes it possible to build a decentralised, incredibly secure system without the need for a central authority to monitor transactions. Blockchain technology, which encrypts data and distributes it over the network, improves information security and privacy and gives governments new chances to increase transparency, stop fraud, and foster citizen confidence. In this paper, we primarily cover the overview of blockchain technology, architecture of blockchain, consensus models and the blockchain use cases in e-Government.***
Keywords: Blockchain, e-Government, Decentralised, peer-to-peer etc.

I. INTRODUCTION

The first cryptocurrency based on blockchain was invented by Satoshi Nakamoto, and it was called Bitcoin [1]. The blockchain technology was first applied to cryptocurrencies. The blockchain acts as an immutable ledger which stores encrypted data. Once the transaction is recorded into blockchain, it cannot be altered in future. Also, blockchain is distributed technology which protect the system from single point of failure condition [1]. Instead of keeping all the data in one place, a central database, blockchain technology can offer more protection by storing data in distributed database. Blockchain shows the prospective to transform traditional industries with its essential characteristics: decentralization, immutability, anonymity, persistency, auditability [2]. Due to its security system, which is appropriate for the information age it can be applied to various other application like healthcare, supply chain, e-government etc.

Blockchain technology can be used by Electronic government (e-government) to improve public administration and enable transparent and secure public services. Information and communication technologies are used by the e-Government to deliver public services to people and companies in an efficient, effective, and transparent way [3]. Personal information about residents is stored by the e-Government services, and this information needs to be appropriately secured from unwanted access. This problem can be solved with blockchain technology since it encourages immutability and transparency of recorded transactions and helps to promote confidence among citizens.

The rest of the paper is ordered as Section II: literature review, Section III: overview of blockchain technology including architecture of blockchain technology, Section IV: Consensus models, Section V: blockchain use cases for e-Government, and finally, Section VI: Conclusion.

II. LITERATURE REVIEW

Nakamoto [1] proposed a system for electronic transactions without trusted third party. The peer-to-peer network solution they showed used proof-of-work to keep track of transactions. If honest nodes dominate CPU power and have created a foundation for currency based on digital signatures, this system is incredibly difficult for an attacker to alter.

Elisa [3] developed a framework for a decentralised e-government system by applying blockchain technology that can guarantee data confidentiality and privacy while also boosting user confidence. Also provided is a prototype of the suggested system.

Park et al. [4] demonstrate the idea of blockchain technology and the research effort surrounding how to actually apply blockchain protection for cloud computing and its secure solutions. They also covered related subjects, such as the fundamentals of blockchain technology and how to use bitcoin as a use case.

Mell et al. [5] discussed the advanced technological overview of blockchain helping readers to know how blockchain technology functions. This paper covers blockchain categorization, blockchain components, forking, applications and limitations.

Zheng et al. [6] presented the broad survey on blockchain technology. In their survey they discussed the blockchain architecture, key characteristics, consensus algorithms used in the blockchain. Later on they analysed the protocols, investigated the typical blockchain applications and listed some challenges and problems.

Finally, concluded with some approaches for solving these problems.

Clavin et al. [7] reviewed blockchain concepts and use cases, and discussed use issues from a government perspective. They reviewed existing and identified use cases of government in the area of healthcare and energy infrastructures along with technical and deployment details of blockchain adoption.

Lykidis et al. [8] reviewed the applications of blockchain technology in e-government to find e-government services that could leverage blockchain. Their intent was to reveal blockchain's potential and contribution to e-government services.

Kassen [9] evaluated the potential advantages and difficulties of automating e-government procedures using blockchain technology. He shared his thoughts on how the technology may be applied to various economic sectors and named the information processes that could be efficiently managed and regulated in blockchain-based networks.

Batubara et al. [10] systematically reviewed the present research topics of blockchain, it's challenges and future directions concerning blockchain acceptance for e-Government. They concluded that the acceptance of blockchain technology in the applications of e-Government is very restricted.

III. OVERVIEW OF BLOCKCHAIN TECHNOLOGY

NIST defines blockchains as "tamper evident and tamper resistant digital ledgers deployed in a distributed form and typically without a central authority." In a blockchain network, a shared ledger can be used by a group of users to create transactions for that group of users, and a published transaction cannot be changed. Bitcoin, the first cryptocurrency to use a blockchain, was created in 2008 [5].

A. Characteristics of Blockchain Technology

The characteristics of blockchain technology are [5]:

1) *Ledger:* To record transactions the blockchain uses append only ledger to ensure that the transactions are not overridden in blockchain network.
2) *Secure:* In a blockchain, the data recorded in the ledger is protected by cryptography, making the data tamper proof.
3) *Sharing:* To create transparency between participants of blockchain network, the ledger is shared by multiple participants.
4) *Distributed:* Because of the distributed characteristic of the blockchain network, it may produce the number of nodes, which makes it more difficult for hostile individuals to attack the system.

B. Types of Blockchain

Blockchain is mainly categorised into following three types [2]:

1) *Public Blockchain:* Public blockchain allows all records to be published and everyone to participate in the consensus process.
2) *Private Blockchain:* The private blockchain is entirely managed by single organization therefore it is assumed as centralized network. In a private blockchain, only nodes belong to a particular organization can take part in the consensus process.
3) *Consortium Blockchain:* The consortium blockchain is considered as decentralized network managed by multiple organizations but only a small portion of nodes can participate in consensus process.

C. Generations of Blockchain technology

Development blockchain technology is an ongoing process categorised into four generations [11]. The comparison among these generations is given in Table I:

1) *First Generation:* The first generation of blockchain technology was introduced in 2009 [11]. The first crypto-currency Bitcoin was developed in this generation.
2) *Second Generation:* The second generation of blockchain technology was introduced in 2010 [11]. In blockchain 2.0, the blockchain technology was extended to smart contracts and financial services for a various applications. In this generation, Ethereum and Hyperledger frameworks were also build up.
3) *Third Generation:* The third generation blockchain technology was introduced in 2015 [11]. In Blockchain 3.0, for blockchain based decentralized applications were developed. To create decentralized applications based on blockchain, a number of study topics have been examined, including health, governance, IoT, supply chain, economics, and smart cities.
4) *Fourth Generation:* The fourth generation blockchain technology was introduced in 2018 [11]. In Blockchain 4.0, the focus was primarily on real time public ledgers and distributed databases. Industry 4.0-based applications of this generation use smart contracts to regulate the network by consensus.

TABLE I: Comparisons of Generations of Blockchain Technology [11]

Generations of Blockchain Technology	1st Generation	2nd Generation	3rd Generation	4th Generation
Known as	Blockchain 1.0	Blockchain 2.0	Blockchain 3.0	Blockchain 4.0
Year of Introduce	2009	2010	2015	2018
Applications	Crypto currency	Smart contract & financial services	Smart contract for decentralised application	Real time public ledgers and distributed databases
Examples	Bitcoin	Ethereum and Hyperledger frameworks	decentralized applications	Industry 4.0 and Healthcare 4.0

D. Blockchain Architecture

A blockchain is a set of blocks that records a list of transactions, similar to traditional public ledger [2]. All the blocks of the blockchain are connected by hash of the previous block. The first block of blockchain which does not have a parent block is called as the Genesis Block. Each block contains some fields that contain information, which is heavily depends on the blockchain network. Figure 1 shows a typical blockchain architecture and chain of blocks [5].

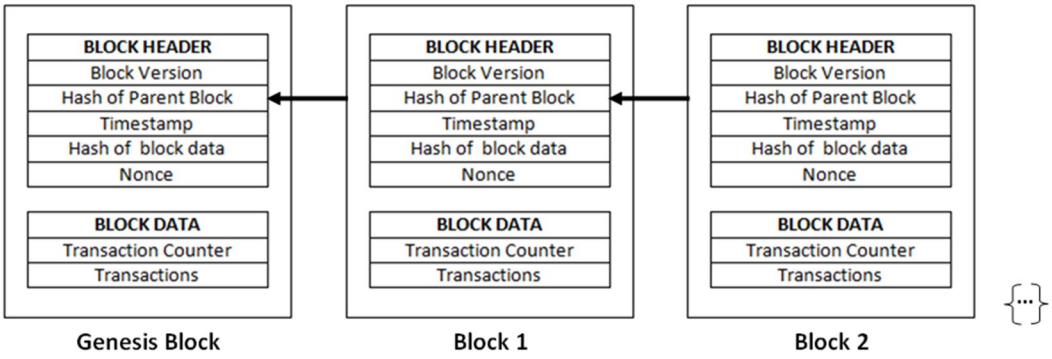


Fig 1: Generic Chain of Blocks

The two primary components of a block are the block header and the block data. The following fields are generally included in the block header. [5]:

1) Block number (version)
2) Hash value of previous block header
3) Timestamp
4) Hash value of block data
5) Nonce value. Nonce is the value that the public node manipulates to solve the hash puzzle in blockchain mining process.

The block data stores the following data [5]:

a) Transaction counter
b) Transactions

IV. CONSENSUS MODELS

An important feature of blockchain technology is to decide who will publish the next block. Such important issue is answered by employing consensus models. In permissionless blockchain networks, several publishing nodes compete to publish the new block simultaneously in order to earn cryptocurrency. Some of consensus models are [5]:

1) *PoW Consensus Model:* In the Proof of Work (PoW) model, the publishing node can published the new block after cracking a rigorous computational puzzle and the solution to the puzzle serves as evidence of their task. The puzzles are made to be challenging to solve, but simple to verify if the solution is valid. As a result, all other perfect nodes may quickly validate all suggested next blocks and reject any that don't solve the puzzle.

2) *PoS Consensus Model:* In the Proof of Stake (PoS) model, the blockchain networks decide who can issue new blocks based on the stake each user has invested. Therefore, the proportion of a blockchain network user's stake to the total cryptocurrency stake of the blockchain network determines the possibility of them releasing a new block.
3) *RR Consensus Model:* In the Round Robin (RR) is a consensus model, the nodes takes turn to form constituents. To deal with scenario where issuing nodes are unable to issue new blocks continuously, the RR systems have a time limit for available nodes to issue new block, ensuring that unavailable nodes do not stop issuing new blocks. This model does not allow single node to creates majority of blocks.
4) *PoA/PoI Consensus Model:* The PoA (Proof of Authority) / PoI (Proof of Identity) consensus model depends on partial trust of public nodes where blockchain network can verify the identity of publishing node and to issue new blocks an issuing node stakes its identity.
5) *PoET Consensus Model:* In the Proof-of-Elapsed-Time (PoET) consensus model, a lottery system is followed giving every node an equal opportunity to win the consensus. Each node on the blockchain network has a random wait time that is generated by the PoET algorithm, and during that time, each node should go to sleep. The node wake up first with the lowest latency will be allowed to write new blocks to the blockchain.

V. BLOCKCHAIN USE CASES IN E-GOVERNMENT

A. Authentication

Pinter et al. [12] suggests using an identification solution built on a blockchain to increase security and availability. They suggest an approach that dispels any concerns about data retention by not storing user data with service providers. Chen et al. [13] suggested using blockchain consensus as a trust transfer paradigm for e-government applications instead of employing conventional trusted third parties. They moved some CA management functions to the blockchain and used consensus to resolve the PKI unified trust service issue nationwide. Paez et al. [14] proposed blockchain-based biometric electronic identification document (e-ID) system for verifying citizens' identities in a variety of transactions involving notarization, registration, tax filing, basic health services, economic activity etc. among others.

B. Data Sharing

Zhang et al. [15] presented a government information exchange model with blockchain as the underlying technology, and use it to solve the security issues, reliability issues, and service customization issues that exist in government information sharing. Liu et al. [16] built a locally differentiated privacy-based framework under blockchain technology to enhance the security, reliability and responsiveness of information sharing. Elisa et al. [17] presented an blockchain enabled e-government architecture to improve security and privacy in the public sector. The recommended system also has the prospective to resolve one of the limitations of existing e-government systems: interoperability between government departments. Xu et al. [18] presented consortium blockchain based ECCS (Electronic Certificate Catalog Sharing) system that is reliable and adaptable, leveraging the immutability and time-stamping of transaction data in the blockchain to advance the accessibility and efficiency of e-government services.

C. e-Voting

Yavuz et al. [19] He used an Ethereum wallet and the Solidity programming language to create and test a sample e-voting application as a smart contract on the Ethereum network. Users can cast their votes immediately from their Ethereum wallet or using an Android device. These transaction requests are handled in accordance with the consensus of all Ethereum nodes, establishing an open environment for electronic voting. Hjalmarsson et al. [20] established a blockchain-enabled electronic voting system based on smart contract that facilitate safe and affordable elections by maintaining voter privacy. A few of the shortcomings of current systems are addressed by the revolutionary blockchain-based electronic voting system. Khan et al. [21] [22] aims to create an efficient system for electronic voting by utilising the benefits of blockchain, such as its cryptographic architecture and transparency. The suggested system is constructed utilising a multi-chain platform that achieves end-to-end verifiability and satisfies the fundamental objectives of e-voting systems.

D. Land Registry

Batubara et al. [23] illustrated how blockchain technology's methods and capabilities may enable transparency and enhance accountability in e-government systems. They demonstrated how blockchain may increase accountability and transparency through a case study of a land register.

Nguyen et al. [24] provided a draught and early test of Vietnam's land valuation certificate management processes that will be blockchain-based. They concentrated on examining the current land appraisal certificate management procedures and the e-government architectural framework of MONRE.

E. Government Contracting

Diallo et al. [25] suggested a Government DAO (eGov-DAO) built on blockchain technology, the first system to allow for real-time monitoring of e-government services. By setting up an affordable, transparent, and secure e-government system, this solution reduces the danger of giving contracts to businesses that are unable to fulfil them.

F. Education

Nespor [26] proposed a blockchain certification platform that enables higher education providers to provide students with official certificates while keeping student information highly confidential. Han et al. [27] used decentralized blockchain technology to create new educational records that could be verified and used to create official certificates. Mitchell et al. [28] created the "dAppER" decentralised application for a review of the examination. Existing procedures are implemented by the decentralised applications, and they are recorded on a blockchain. The distinction is that this documentation is immutable and irreversible, making it very suitable for auditability.

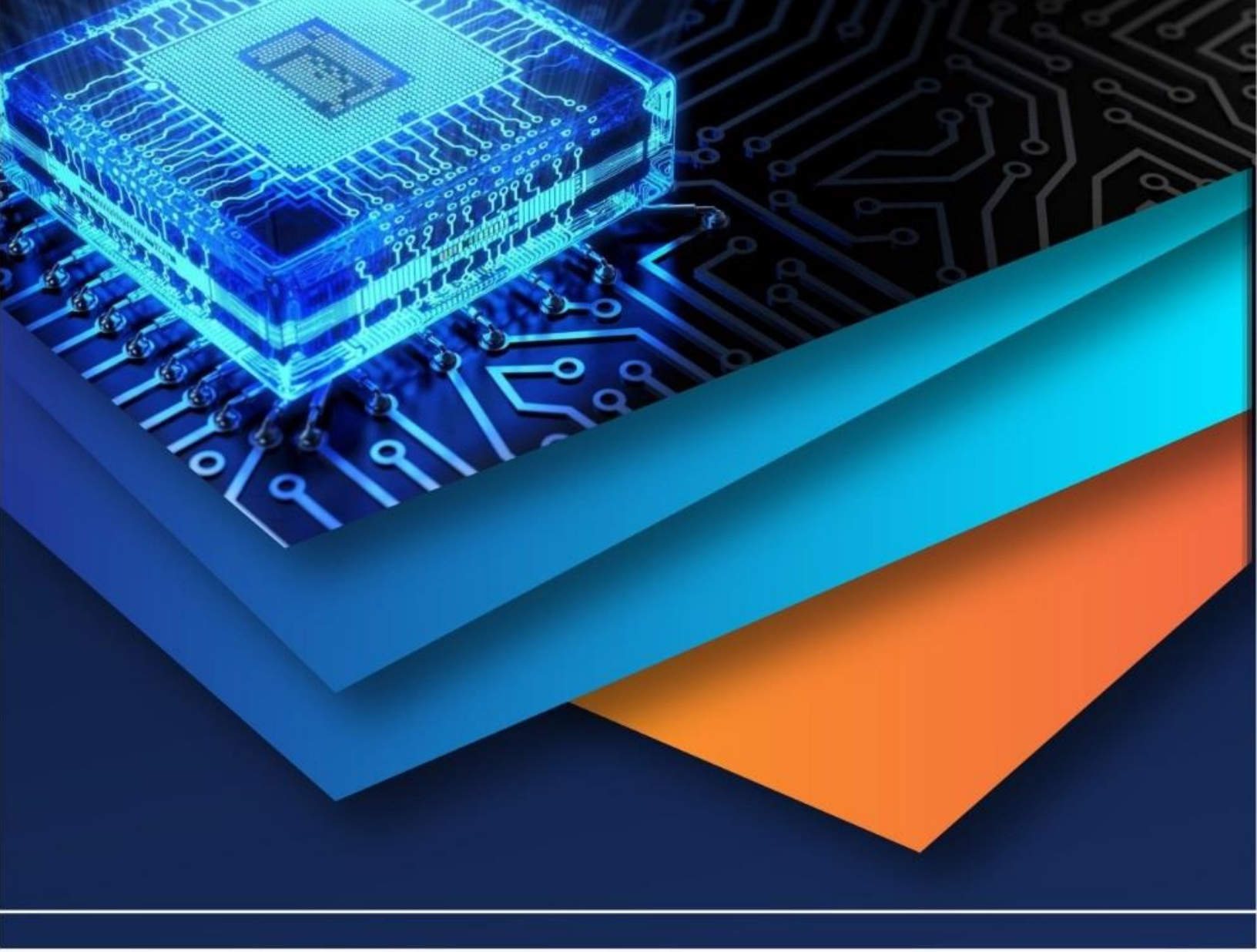
VI. CONCLUSION

The majority of the current e-government systems are centralised on redundant servers and databases, leaving them susceptible to single points of failure and making them open to cyberattacks. Compared to keeping all of your data in a single database, blockchain can offer more security. Blockchain is a distributed, unchangeable ledger that is used to keep track of transactions, assets, and establish trust. Immutable property makes it impossible for any entity to tamper with, replace, or forge data stored on the network. Blockchain technology, where data is encrypted and distributed over the network, enhances information security and privacy and gives governments new chances to increase transparency, stop fraud, and promote citizen confidence. The use cases discussed here shows that blockchain offers many possible opportunities in e-Government system. So far, blockchain technology is mainly used for cryptocurrencies, digital contracts, supply chain etc. The future applications are expected to extend to full-fledged e-Government system.

REFERENCES

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.
[2] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” Proc. - 2017 IEEE 6th Int. Congr. Big Data, BigData Congr. 2017, pp. 557–564, 2017.
[3] N. Elisa, L. Yang, F. Chao, and Y. Cao, “A framework of blockchain-based secure and privacy-preserving E-government system,” Wirel. Networks, vol. 0, 2020.
[4] J. H. Park and J. H. Park, “Blockchain security in cloud computing: Use cases, challenges, and solutions,” Symmetry (Basel)., vol. 9, no. 8, pp. 1–13, 2017.
[5] D. Yaga, P. Mell, N. Roby, and K. Scarfone, “Blockchain Technology Overview,” National Institute of Standards and Technology Internal Report 8202. 2018.
[6] H. Wang, Z. Zheng, S. Xie, H. N. Dai, and X. Chen, “Blockchain challenges and opportunities: a survey,” Int. J. Web Grid Serv., vol. 14, no. 4, p. 352, 2018.
[7] J. Clavin et al., “Blockchains for Government,” Digit. Gov. Res. Pract., vol. 1, no. 3, pp. 1–21, 2020.
[8] I. Lykidis, G. Drosatos, and K. Rantos, “The use of blockchain technology in e-government services,” Computers, vol. 10, no. 12, pp. 1–17, 2021.
[9] M. Kassen, “Blockchain and e-government innovation: Automation of public information processes,” Inf. Syst., vol. 103, p. 101862, 2022.
[10] F. R. Batubara, J. Ubacht, and M. Janssen, “Challenges of blockchain technology adoption for e-government: A systematic literature review,” ACM Int. Conf. Proceeding Ser., 2018.
[11] U. Bodkhe et al., “Blockchain for Industry 4.0: A comprehensive review,” IEEE Access, vol. 8, pp. 79764–79800, 2020.
[12] K. Pinter, D. Schmelz, R. Lamber, S. Strobl, and T. Grechenig, “Towards a Multi-party, Blockchain-Based Identity Verification Solution to Implement Clear Name Laws for Online Media Platforms,” Lect. Notes Bus. Inf. Process., vol. 361, pp. 151–165, 2019.
[13] Y. Chen, G. Dong, J. Bai, Y. Hao, F. Li, and H. Peng, “Trust enhancement scheme for cross domain authentication of PKI system,” Proc. - 2019 Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discov. CyberC 2019, pp. 103–110, 2019.
[14] R. Páez, M. Pérez, G. Ramírez, J. Montes, and L. Bouvarel, “An architecture for biometric electronic identification document system based on blockchain,” Futur. Internet, vol. 12, no. 1, pp. 1–19, 2020.
[15] Y. Zhang, S. Deng, Y. Zhang, and J. Kong, “Research on government information sharing model using blockchain technology,” Proc. - 10th Int. Conf. Inf. Technol. Med. Educ. ITME 2019, pp. 726–729, 2019.
[16] L. Liu, C. Piao, X. Jiang, and L. Zheng, “Research on Governmental Data Sharing Based on Local Differential Privacy Approach,” Proc. - 2018 IEEE 15th Int. Conf. E-bus. Eng. ICEBE 2018, pp. 39–45, 2018.
[17] N. Elisa, L. Yang, H. Li, F. Chao, and N. Naik, “Consortium blockchain for security and privacy-preserving in E-government Systems,” Proc. Int. Conf. Electron. Bus., vol. 2019-Decem, pp. 99–107, 2019.

[18] C. Xu, H. Yang, Q. Yu, and Z. Li, "Trusted and Flexible Electronic Certificate Catalog Sharing System Based on Consortium Blockchain," IEEE Xplore, 2020.
[19] A. K. Koç, E. Yavuz, U. C. Çabuk, and G. Dalkiliç, "Towards secure e-voting using ethereum blockchain," 6th Int. Symp. Digit. Forensic Secur. ISDFS 2018 - Proceeding, vol. 2018-January, pp. 1–6, 2018.
[20] F. P. Hjalmarsson, G. K. Hreioarsson, M. Hamdaqa, and G. Hjalmtysson, "Blockchain-Based E-Voting System," IEEE Int. Conf. Cloud Comput. CLOUD, vol. 2018-July, pp. 983–986, 2018.
[21] K. M. Khan, J. Arshad, and M. M. Khan, "Investigating performance constraints for blockchain based secure e-voting system," Futur. Gener. Comput. Syst., vol. 105, pp. 13–26, 2020.
[22] K. M. Khan, J. Arshad, and M. M. Khan, "Secure digital voting system based on blockchain technology," Int. J. Electron. Gov. Res., vol. 14, no. 1, pp. 53–62, 2018.
[23] F. Rizal Batubara, J. Ubacht, and M. Janssen, "Unraveling transparency and accountability in blockchain," ACM Int. Conf. Proceeding Ser., pp. 204–213, 2019.
[24] N. H. Nguyen, B. M. Nguyen, T. C. Dao, and B. L. Do, "Towards Blockchainizing Land Valuation Certificate Management Procedures in Vietnam," Proc. - 2020 RIVF Int. Conf. Comput. Commun. Technol. RIVF 2020, 2020.
[25] N. Diallo et al., "EGov-DAO: A Better Government using Blockchain based Decentralized Autonomous Organization," 2018 5th Int. Conf. eDemocracy eGovernment, ICEDEG 2018, pp. 166–171, 2018.
[26] J. Nespor, "Cyber schooling and the accumulation of school time," Pedagog. Cult. Soc., vol. 27, no. 3, pp. 325–341, 2019.
[27] M. Han, D. Wu, Z. Li, Y. Xie, J. S. He, and A. Baba, "A novel blockchain-based education records verification solution," SIGITE 2018 - Proc. 19th Annu. SIG Conf. Inf. Technol. Educ., pp. 178–183, 2018.
[28] I. Mitchell, S. Hara, and M. Sheriff, "dAppER : D ecentralised App lication for E xamination R eview," 2019 IEEE 12th Int. Conf. Glob. Secur. Saf. Sustain., pp. 1–14, 2019.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY