

# Secure Framework For Government Delicate Assignment

Ms. Demel Abisha<sup>1</sup>, Veeramani M<sup>2</sup>, Sathish K<sup>3</sup>, Udithkumar E<sup>4</sup>

Assistant Professor, Department of Computer Science<sup>1</sup>

Students, Department of Computer Science<sup>2,3,4</sup>

Dhanalakshmi College of Engineering, Chennai, India

**Abstract:** Block chain innovation isan representation of such innovation that has been attracting in the consideration of Legislatures throughout the globe. Upgraded security, further developed detectability, and most minimal expense foundation engage the block chain to enter different areas. By and large, legislatures discharge tenders to some outsider associations for various tasks. During this interaction, various contenders attempt to snoop the delicate upsides of others to win the delicate. Block chain strategy utilized under different security administration with various model. It is utilized as backend data set model that keeps up with. No. of clients can enlist and make the delicate citation under different division. Administrator will check and give the reaction from the citation result. Administrator or authority check the experience and interaction the executives level expertise for broadly useful.

**Keywords:** Blockchain, digital signatures, secure hash algorithm, edge computing, proof of work, smart contracts and smart tenders.

## I. INTRODUCTION

There have been different endeavors to carry out the innovation to make government processes paperless and immediate, for example, web based tagging frameworks, internet giving of tenders, documenting expense forms, and so on. Albeit a large portion of these frameworks appear to be hearty and very much carried out, every one of them depend on the possibility of a focal server that has a weak link, as programmers can undoubtedly hack or disturb its working by assaults, like DOS, Slow-loris, SYN Flooding, and so forth. In many states, convoluted administrative frameworks frequently bring about exceptionally wasteful work process laden with debasement, bungle, and human blunders. A portion of the administration processes, for example, government tenders incorporate misbehaviors like data spills, debasement, pay off, and so on. The greater part of the current electronic administrations and IT foundation have the previously mentioned limits, be that as it may, new advances, for example, blockchain can possibly incredibly improve the current issues. Current e-tendering processes aren't 'fair and open,' which means that information isn't shared with all parties involved. When a corporation is chosen as the winner of a contract, for example, the information is disseminated 'as they wish. Organizations that bid on a same tender aren't told why their proposal was rejected or why one company was chosen as the winner. A corporation can request this information, but obtaining it is a time-consuming process. Even if you can confirm these documents, it takes time to confirm. A side from not being transparent, the security of these portals is a major worry, as it can lead to fraud and data manipulation in a central database. If a hacker acquires access to this central database, bids can be shared with competitors, resulting in severe financial and strategic losses for a corporation. Blockchain technology addresses these security concerns as it primarily focuses on the decentralization of information, protected by cryptography combined with an irrefutable block-based architecture for transaction management. As a consequence, Blockchain and Smart Contracts may be used to construct a transparent, decentralized, and secure tendering framework that allows bidders to keep track of portal functionality and all tender portal activity. RFPs or contracts are often used by governments and businesses to procure goods and services. Wrong bid management leads to huge losses in case of bad practices.

## II. LITERATURE REVIEW

**H. Cho, "Correction to ASIC-resistance of multi-hash proof-of-work mechanisms for blockchain consensus protocols," IEEE Access, vol. 7, 2019, Art. no. 25086**

Blockchain technology has quickly gained popularity due to its decentralized and open operation. The consensus protocol is the central mechanism of securing the assigned ledger from potential adversary attacks in a blockchain community. Proof-of-work (PoW) is a popular consensus process that necessitates a substantial quantity of computation to identify a new legitimate block. The decentralized feature of blockchain networks is endangered when application-specific integrated circuits (ASICs) designed specifically for PoW computation grow to dominate the blockchain consensus process. Many PoW strategies are being developed in order to discourage the usage of ASICs in consensus operations. One of the often-used techniques to achieve such ASIC-resistance is to use more than one hash feature in the PoW computation that is multi-hash PoW. The degree of ASIC resistance of multi-hash PoW processes is empirically investigated in this work. The overall performance difference between ASICs and general-purpose computer systems is used to determine the amount of ASIC resistance. Our findings show that the ASIC-resistance of various PoW mechanisms is no longer powerful enough to prevent ASIC-based mining, contrary to the assumptions of multihashPoW techniques. The majority of them contain ASIC-resistance layers that are comparable to PoW techniques that have already been beaten by ASIC-based systems.

**V. Hassija, V. Chamola, S. Garg, N. G. K. Dara, G. Kaddoum, and D. N. K. Jayakody, "A blockchain-based framework for light-weight records sharing and power buying and selling in V2G network," IEEE Trans. Veh. Technol., vol. 60, no. 6, pp. 5799–5812, Jun. 2020**

The Vehicle-to-Grid (V2G) community, which uses battery-powered cars to feed electricity into the power grid, is exploding. In a V2G community, a scalable, stable and cost-effective system is necessary to support the growing number of transactions. Existing studies rely on standard blockchain to meet this need. Because the mining incentive is bigger than the transaction cost, blockchain-enabled V2G networks demand a lot of computing power and are no longer suitable for micro-transactions. Furthermore, standard blockchain transaction throughput is insufficient to serve the growing volume of traditional transactions on V2G networks. To overcome these challenges, this research offers the Directed Acyclic Graph-based V2G community, a lightweight blockchain-based protocol (DV2G). The term "blockchain" is used in this context to refer to any Distributed Ledger Technology (DLT), not simply the bitcoin block chain. To document community transactions in a strictly closed and scalable manner, a tangle information shape is being used

## III. PROPOSED SYSTEM

A permissioned block chain network will provide the transparency required to efficiently implement government regulations for the advantage of the country's population while also establishing obligations in the event of system misuse.

## IV. IMPLEMENTATION

### Public Complaint

In this module in our project, Public add complaint something about some issues about his/her area or zone such as water department issue, Electricity related issue with the picture of that.

### Department Register

In this module the department has to register with user name and password along with the name of the department. This register data stored in the database.

### Department Login

In this module in our project, Department admin has to login with user id and password if they are valid then the admin will redirect to respective department view.

### Select Department

In this module in our project, here the department is need to select the department like construction or some department for the tender allocation.

### Department Upload

In this module, the respective department will upload the public complaint along with all the details in PDF file format to the Government. Here we are encrypting the file with AES. When the government wants to see the file, it will be decrypted.

### Government Login

In this module of our project, Government admin has to login with user id and password if they are valid then the admin will redirect to government view.

### Government View

In this module the government will also view the contractor. And analysis the details will be responsible for your file stored in database.

### Government Tender Allocation

In this module the government will allocate the tender for the government Analysis the details will be responsible for your file stored in database.

### Government Approve

Government Approve module is used to assist the contractor in requesting the tender with the land longitude, and the contractor will update the report with their opinion, which will be saved in the database.

### Contractor Register

In this module, the contractor has to register in order to see the tender. In the registration page contractor has to fill all the details of the company along with username and password. All the details will go to the government admin. The admin will see all the details of the company if it is a legal and valid company then admin will accept otherwise admin will reject.

### Contractor Login

In this module the contractor will get the login credentials if the government admin accepts the request. The contractor can then login with his/her credentials.

### Contractor Tender Request

In this module the contractor will also view the request. And analysis the details will be responsible for your file stored in database.

### Contractor Appointment

In this module is used to help to the contractor to request the tender with the appointment by the government and the contractor will update the report along with their opinion and they will be stored the database.

### Algorithm

SHA 256 is a part of the SHA 2 family of algorithms, where SHA stands for Secure Hash Algorithm. Published in 2001, it was a joint effort between the NSA and NIST to introduce a successor to the SHA 1 family, which was slowly losing strength against brute force attacks. The significance of the 256 in the name stands for the final hash digest value, i.e. irrespective of the size of plaintext/cleartext, the hash value will always be 256 bits.

**Algorithm Characteristics**

**Message Length:** The length of the cleartext should be less than 264 bits. The size needs to be in the comparison area to keep the digest as random as possible.

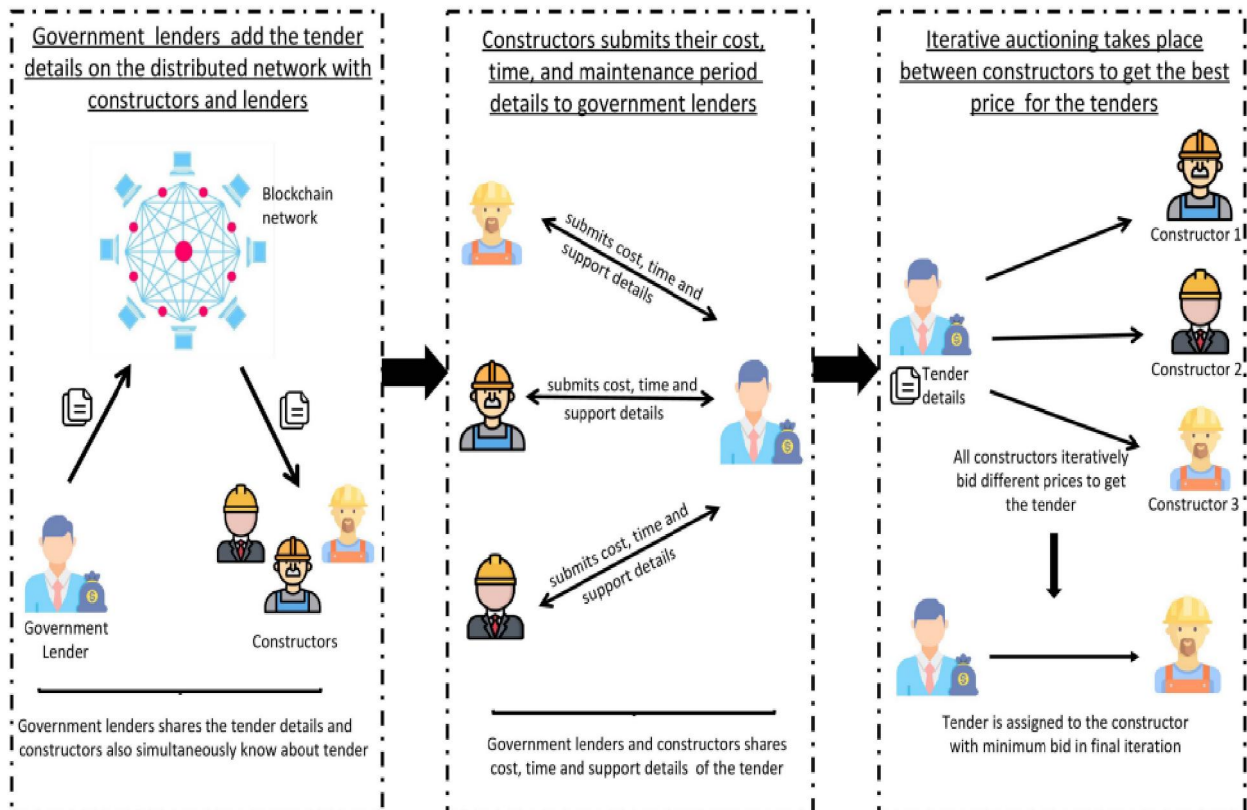
**Digest Length:** The length of the hash digest should be 256 bits in SHA 256 algorithm, bits in SHA-512, and so on. Bigger digests usually suggest significantly more calculations at the cost of speed and space.

**Irreversible:** By design, all hash functions such as the SHA 256 are irreversible. You should neither get a plaintext when you have the digest beforehand nor should the digest provide its original value when you pass it through the hash function again

**Applications:**

- **Digital Signature Verification:** Digital signatures follow asymmetric encryption methodology to verify the authenticity of a document/file. Hash algorithms like SHA 256 go a long way in ensuring the verification of the signature.
- **Password Hashing:** As discussed above, websites store user passwords in a hashed format for two benefits. It helps foster a sense of privacy, and it lessens the load on the central database since all the digests are of similar size.
- **SSL Handshake:** The SSL handshake is a crucial segment of the web browsing sessions, and it's done using SHA functions. It consists of your web browsers and the web servers agreeing on encryption keys and hashing authentication to prepare a secure connection.
- **Integrity Checks:** As discussed above, verifying file integrity has been using variants like SHA 256 algorithm and the MD5 algorithm. It helps maintain the full value functionality of files and makes sure they were not altered in transit

**IV. RESULTS AND DISCUSSION**



**Fig1:** Proposed framework's step-by-step flow  
DOI: 10.48175/568

**complainer Details**

Full Name  Email Address

Address

Compliant Date  Mobile Number

**Compliant Location And Type of Compliant**

Zone

Compliant Department

Compliant Type

Street  Compliant Description minimum of words

Fig 2: Police Complaint Form

DEPARTMENT	DATE	ZONE	COMPLAINT	COMPLIANT STREET	REPORT	FINISH
WATER MANAGEMENT	2022-02-02	TONDIARPET	pls supply drinking water	12 th street tondiarpet	VIEW	Done

Fig 3: Complaint Status on Government view Page

DEPARTMENT	DATE	ZONE	PROJECT	AMOUNT	DURATION	VIEW	REQUEST
WATER MANAGEMENT	2022-02-05	ANNA NAGAR	sample.pdf	1000000	3 months	VIEW	REQUEST

Fig 4: Tender Request on Contractor view page

CONTRACT COMAPNY	DEPARMENT NAME	DATE	ZONE	ALLOCATE AMOUNT	DURATION	REQUEST AMOUNT	ACCEPT	Rejected
cts	WATER MANAGEMENT	2022-03-04T14:57	GUNTUR	9000000	2 months	9500000	APPROVED	REJECT

Fig 5: Tender Response on Government View page.



Zone	Address	Department	Company Name	Project Details	Duration	Allocate Date	Total Cast
THIRUVOTRIYUR	Gandhi Nagar	WATER MANAGEMENT	abb corparation	link.txt	6 months	2022-02-02T17:49	110000
MANALI	12 th street tondiarpet	ROAD SECTOR	abb corparation	Dilation, Erosion, Opening and Closing.txt	3 months	2022-02-02T17:58	1300000
PERUNGUDI	2nd street annanagar	WATER MANAGEMENT	jk construction	Edge Detection & Image Gradients.txt	3 months	2022-02-02T18:04	90000
TONDIARPET	1 st tondiarpet quartus	ROAD SECTOR	bb corparation	sample.pdf	3 months	2022-02-04T17:35	1100000

**Fig 6: Allocated Tender Details on Government view Page.**

## V. CONCLUSION

In this article, we have talked about on the need and advantages of utilizing block chain innovation in the public authority delicate task process. We have used to execute the start to finish edge processing system for an administration delicate work process. The sha calculation is proposed to relate the most appropriate constructors to the delicate undertakings, subsequently improving the benefit of both the public authority tenders and the development organizations. We have likewise concentrated on the presentation assessment of the proposed model. The proposed model demonstrates to give improved brings about terms of various delicate boundaries when contrasted with its partners.

## VI. FUTURE ENHANCEMENTS

Improving protocol efficiency, both in terms of the number of tenders exchanged and in terms of time. Implementing using two are more algorithms

## REFERENCES

- [1]. V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.
- [2]. A. Alketbi, Q. Nasir, and M. A. Talib, "Blockchain for government services—Use cases, security benefits and challenges," in *Proc. IEEE 15th Learn. Technol. Conf. (L&T)*, 2018, pp. 112–119. 2418 *IEEE INTERNET OF THINGS JOURNAL*, VOL. 8, NO. 4, FEBRUARY 15, 2021
- [3]. coindesk. The Indian Government Is Preparing a National Framework to Support the Wider Deployment of Blockchain Use Cases. Accessed: Nov. 27, 2019. [Online]. Available: <https://www.coindesk.com/indiaplans-to-issue-a-national-blockchain-framework>
- [4]. H. Cho, "Correction to asic-resistance of multi-hash proof-of-work mechanisms for blockchain consensus protocols," *IEEE Access*, vol. 7, 2019, Art. no. 25086.
- [5]. V. Hassija, V. Chamola, S. Garg, N. G. K. Dara, G. Kaddoum, and D. N. K. Jayakody, "A blockchain-based framework for lightweight data sharing and energy trading in V2G network," *IEEE Trans. Veh. Technol.*, vol. 60, no. 6, pp. 5799–5812, Jun. 2020.
- [6]. V. Hassija, V. Chamola, D. N. G. Krishna, and M. Guizani, "A distributed framework for energy trading between UAVs and charging stations for critical applications," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 5391–5402, May 2020.
- [7]. E. Androulaki et al., "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. ACM 13th EuroSys Conf.*, 2018, p. 30.
- [8]. V. Hassija, V. Chamola, G. Han, J. J. Rodrigues, and M. Guizani, "DAGIoV: A framework for vehicle to vehicle communication using directed acyclic graph and game theory," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 4182–4191, Jan. 2020.
- [9]. C. D. Clack, V. A. Bakshi, and L. Braine, "Smart contract templates: Essential requirements and design options," 2016. [Online]. Available: [arXiv:1612.04496](https://arxiv.org/abs/1612.04496).

- [10]. C. Cachin, "Architecture of the hyperledger blockchain fabric," in Proc. Workshop Distrib. Cryptocurrencies Consensus Ledgers, 2016, p. 310.
- [11]. H. Cho, "Asic-resistance of multi-hash proof-of-work mechanisms for blockchain consensus protocols," IEEE Access, vol. 6, pp. 66210–66222, 2018.
- [12]. J. D. Groot. The History of Data Breaches. Accessed: Oct. 24, 2019. [Online]. Available: <https://digitalguardian.com/blog/history-databreaches>
- [13]. M. C. K. Khalilov and A. Levi, "A survey on anonymity and privacy in bitcoin-like digital cash systems," IEEE Commun. Surveys Tuts., vol. 20, no. 3, pp. 2543–2585, 3rd Quart., 2018.
- [14]. J. A. Jaoude and R. G. Saade, "Blockchain applications—Usage in different domains," IEEE Access, vol. 7, pp. 45360–45381, 2019.
- [15]. H. Hou, "The application of blockchain technology in e-government in china," in Proc. IEEE 26th Int. Conf. Comput. Commun. Netw. (ICCCN), 2017, pp. 1–4.
- [16]. S. Ølnes and A. Jansen, "Blockchain technology as S support infrastructure in e-government," in Proc. Int. Conf. Electron. Govt., 2017, pp. 215–227.
- [17]. S. Ølnes, "Beyond bitcoin enabling smart government using blockchain technology," in Proc. Int. Conf. Electron. Govt., 2016, pp. 253–264.
- [18]. S. Rama, S. V. Flowerday, and D. Boucher, "Information confidentiality and the chinese wall model in government tender fraud," in Proc. IEEE Inf. Security South Africa, 2012, pp. 1–8.
- [19]. A. Dello and C. Yoshida, "Online tendering and evaluation for public procurement in tanzania," in Proc. 18th IEEE/ACIS Int. Conf. Softw. Eng. Artif. Intell. Netw. Parallel Distrib. Comput. (SNPD), 2017, pp. 137–141.
- [20]. Z. Hui and J. Yang, "Research on application of e-Tender in China," in Proc. IEEE Int. Conf. Internet Technol. Appl., 2011, pp. 1–3.
- [21]. H. Fukui and K. Kobayashi, "Optimal comprehensive tendering models for project procurement," in Proc. IEEE Int. Conf. Syst. Man Cybern., 2010, pp. 3258–3264.
- [22]. P. Dunphy and F. A. P. Petitcolas, "A first look at identity management schemes on the blockchain," IEEE Security Privacy, vol. 16, no. 4, pp. 20–29, Aug. 2018.
- [23]. Q. Lin, H. Yan, Z. Huang, W. Chen, J. Shen, and Y. Tang, "An IDbased linearly homomorphic signature scheme and its application in blockchain," IEEE Access, vol. 6, pp. 20632–20640, 2018.
- [24]. C. Lin, D. He, X. Huang, M. K. Khan, and K.-K. R. Choo, "A new transitively closed undirected graph authentication scheme for blockchain-based identity management systems," IEEE Access, vol. 6, pp. 28203–28212, 2018.
- [25]. P. Noizat, "Blockchain electronic vote," in Handbook of Digital Currency. Amsterdam, The Netherlands: Elsevier, 2015, pp. 453–461.
- [26]. Y. Zhang, S. Deng, Y. Zhang, and J. Kong, "Research on government information sharing model using blockchain technology," in Proc. IEEE 10th Int. Conf. Inf. Technol. Med. Educ. (ITME), 2019, pp. 726–729.
- [27]. S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F. Wang, "Blockchainenabled smart contracts: Architecture, applications, and future trends," IEEE Trans. Syst., Man, Cybern., Syst., vol. 49, no. 11, pp. 2266–2277, Nov. 2019.
- [28]. M. O'Neill and M. J. B. Robshaw, "Low-cost digital signature architecture suitable for radio frequency identification tags," IET Comput. Digit. Techn., vol. 4, no. 1, pp. 14–26, Jan. 2010.
- [29]. R. Rosa and C. E. Rothenberg, "Blockchain-based decentralized applications for multiple administrative domain networking," IEEE Commun. Stand. Mag., vol. 2, no. 3, pp. 29–37, Sep. 2018
- [30]. B. K. Mohanta, S. S. Panda, and D. Jena, "An overview of smart contract and use cases in blockchain technology," in Proc. 9th Int. Conf. Comput. Commun. Netw. Technol. (ICCCNT), Jul. 2018, pp. 1–4.
- [31]. J. Huang, L. Kong, G. Chen, M.-Y. Wu, X. Liu, and P. Zeng, "Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism," IEEE Trans. Ind. Informat., vol. 15, no. 6, pp. 3680–3689, Jun. 2019.
- [32]. V. Hassija, V. Saxena, V. Chamola, and R. Yu, "A parking slot allocation framework based on virtual voting and adaptive pricing algorithm," IEEE Trans. Veh. Technol., vol. 60, no. 6, pp. 5945–5957, Jun. 2020.

- [33]. V. Hassija, V. Saxena, and V. Chamola, "A mobile data offloading framework based on a combination of blockchain and virtual voting," *Softw. Pract. Exp.*, to be published.
- [34]. N. G. Saglam, A. Z. Yilmaz, C. Becchio, and S. P. Corgnati, "A comprehensive cost-optimal approach for energy retrofit of existing multi-family buildings: Application to apartment blocks in Turkey," *Energy Build.*, vol. 150, pp. 224–238, Sep. 2017.
- [35]. C. Yang, C. Liu, X. Zhang, S. Nepal, and J. Chen, "A time efficient approach for detecting errors in big sensor data on cloud," *IEEE*