

# BLOCKCHAIN-BASED E-VOTING SYSTEM

P. Ashrin Ummu Salma

Department of Information Technology,

Francis Xavier Engineering College,

103/G2, Bypass Road Vannarpettai, Tirunelveli, Tamil Nadu-627003

ashrinummusalma20@gmail.com

## ABSTRACT

*It's been difficult for legislators to create an electronic voting system that meets legal criteria for a long time. In the field of information technology, distributed ledger systems represent an exciting technological advancement. An endless number of applications that profit from sharing economies are possible with block chain technologies. The purpose of this article is to assess how distributed electronic voting systems can be implemented using blockchain technology. The suggested block chain-based electronic voting system uses a permissioned block chain with separate nodes for voters, election authorities, and validators, and it makes use of SHA-256 for safe data integrity. The voting procedure, vote encryption, and voter eligibility are all managed by the system through smart contracts. Encrypting voter data, using biometric or digital identity verification, and using secure digital interfaces are all part of the voting process. Each vote is guaranteed to be distinct and authentic by the use of SHA256, and the block chain offers immutability and transparency. Encrypting voter data, avoiding duplicate voting, managing keys securely, and conducting frequent security audits are examples of security procedures.*

## 1. INTRODUCTION

A block chain is an expanding list of records connected by encryption, known as blocks. Each block has transaction data, a timestamp, and a cryptographic hash of the block before it. For the purpose of the hash, the timestamp verifies that the transaction data was there at the time the block was released. Blocks create a chain because they are interconnected and reinforce each other since they each hold information about the block that came before it. Because once recorded, the data in any given block cannot be changed retrospectively without changing all following blocks, block chains are resistant to data tampering. In order to function as a publicly distributed ledger, block chains are usually maintained by a peer-to-peer network, in which nodes cooperate to exchange messages and verify new blocks. While forks may cause records on a block chain to become unchangeable, block chains are secure by design and represent a distributed computing system with strong Byzantine fault tolerance. Based on work by Stuart Haber, W. Scott Stornetta, and Dave Bayer, the block chain was as made popular in 2008 by a person (group of persons) going by the name Satoshi Nakamoto to operate as the public

transaction log of the cryptocurrency bitcoin. To this Satoshi Nakamoto's identity is a mystery. Due to the block chain's integration, bitcoin is the First virtual currency that can prevent double spending without the aid of a central server or dependable authority. Other publicity viewable application and block chains that are extensively utilised by cryptocurrencies have been influenced by the data of the bitcoin. The block chain is seen as a particular kind of payment rail.

## 2. LITERATURE REVIEW

Devices it has been suggested by Weitian Tong [1] et al. This paper discusses how social media platforms of today unite individuals and make it easier to plan different kinds of group activities. The ability to infer the activity habits of wearable smart gadgets' owners has also been made possible by their quick development. We create a clever and private social activity invitation framework using historical data from smart devices, drawing inspiration from the latest work by Ai et al. Our paradigm seeks to assist users in planning group activities in a clever and effective manner while identifying middle ground that satisfies all stakeholders. Our approach,

which requires users to provide their personal information to the app server in order for it to organise services for registered members, is more practical than Ai et al.'s work. But the app server is suspicious and might be driven by things like advertising money. In order to draw in new users, the app might therefore market itself by offering aggregate statistical data about its present user base.

This puts the goals of the app creators at odds with the worries about personal privacy held by the current user base. Our architecture resolves this contradiction by providing state-of-the-art privacy protection (differential privacy) for the information of current users, ensuring high-quality services for current users and enabling the server to provide informative responses to new potential users. Furthermore, the suggested system employs a novel technique based on perturbed graphs to incentivize inactive or solitary users. In this work, Meng han [2] Many different kinds of network applications contain imprecision, incompleteness, and dynamic elements. Determining the uncertainty relationship between nodes is challenging since typical models do not apply to uncertain networks, and problems with uncertainty always have unmanageable computing complexity. In this paper, we model a series of network snapshots to an uncertain graph in order to examine how to capture the uncertainty in networks. A framework is introduced to convert uncertain networks into deterministic weight networks, where the weights on edges can be measured as a Jaccard-like index. This is made possible by the novel sampling scheme that is proposed, which allows for the development of an efficient algorithm to measure in uncertain networks. The framework takes into consideration the practicality of neighbourhood relationships in real networks. The thorough experimental assessment on actual data shows how effective and efficient our algorithms are. This study offers the following contributions in response to the aforementioned difficulties. Initially, a useful technique for modelling uncertainty is to use a static model with a few extra features to simulate a network's dynamic feature. As a result, we provide two fundamental models for various applications that represent uncertainty in dynamic networks. These two models forecast future relationships based on historical data. Secondly, we use the sampling technique to handle uncertain possible worlds due to the high cost of handling and mining uncertainty. Moreover, the precision of the results obtained is ensured by applying the Hoeffding

inequality and the Chernoff bound.

Jakob Gawlikowski, [3] among others, has suggested. In this work Neural networks have permeated practically every scientific discipline in the past ten years and are now an essential component of numerous real-world applications. The significance of neural network predictions' trust grew as they spread more widely. Nevertheless, simple neural networks are ill-calibrated because they cannot provide certainty estimates or exhibit excessive or insufficient confidence. To get around this, a lot of academics have been figuring out how to measure and comprehend prediction uncertainty in neural networks. This has led to the identification of several forms and causes of uncertainty as well as the proposal of numerous methods for measuring and quantifying uncertainty in neural networks. This article provides a thorough introduction to neural network uncertainty estimation, discusses recent developments in the subject, outlines existing issues, and suggests future directions for investigation. It does not assume any prior expertise in this area and is meant to provide a general overview and introduction to anyone interested in uncertainty estimates in neural networks. In order to achieve this, a thorough overview of the most important sources of uncertainty is provided, along with a division of those sources into categories such as reducible model uncertainty and non-reducible data uncertainty. Several areas of these fields are reviewed, along with the most recent advancements, in the modelling of these uncertainties based on deterministic neural networks, Bayesian neural networks, ensembles of neural networks, and testtime data augmentation techniques. We address various uncertainty measures, neural network calibration techniques, and provide an overview of current baselines and implementations for a realistic application.

Wang Yingjie [4] et al. have suggested. In this work We carry out related experiments in this section to assess the efficacy of the suggested incentive scheme. Firstly, we compare TATP with various traditional auction algorithms to confirm its efficiency. Then, two data sets of cab movement traces from Beijing and New York are used to confirm the efficacy of the suggested privacy-preserving method. Every experiment was carried out using the Matlab 7.0 simulation platform, an Intel Core (TM) Duo 2.66 GHz CPU, 12GB of RAM, and the Windows 10 operating

Genuine incentive system. In order to encourage employees to participate in activities and behave honestly, the study investigated an enhanced two-stage auction algorithm based on true degree and privacy degree (TATP). The K-differential privacy-preserving method was proposed by merging the techniques of different privacy preserving and k-anonymity privacy preserving to safeguard the privacy of workers' whereabouts.

Among others, Albin Benny [5] has suggested. In this essay, we'll discuss how technology is now widely used to help meet human needs. Elections are crucial in modern democracies because of the growing mistrust that the majority of people have for their governments as a result of the growing usage of technology. Elections are crucial in deciding who will lead a country or organisation, or one could argue that they are a momentous occasion that determines the destiny of any given nation. Elections are crucial to modern democracies, but a key problem for democracy is that a sizable portion of the global populace does not trust their electoral process. Even the biggest democracies in the world, such as the United States and India, still have problems with their voting processes. The main problems with the existing voting system are polling booth capturing, election manipulation, vote rigging, and hacking of electronic voting machines (EVMs). According to some, block chain technology is a decentralised, distributed, and growing technology that has the potential to improve numerous industries. One way to address the current issues with the e-voting system could be to include block chain technology into the voting process. Undoubtedly, the dynamic nature of the block chain, the foundation of the well-known cryptocurrency Bitcoin, has ushered in a new era for the Internet and block chain services. Although the majority of people only pay attention to bitcoin and other cryptocurrencies, many administrative and finance tasks that were previously only possible offline or on a block chain can now be safely brought online as block chain services due to the immutability of block chain technology. Block chain's numerous features and smart contracts, which outperform conventional systems, are what make it such a potent tool. Meaningful code segments known as "smart contracts" are to be incorporated into the block chain and run on a predetermined timetable during each stage of block chain updates. Another important yet currently

popular topic pertaining to block chain services is e-voting. Smart contract-enabled block chains show promise for usage in the creation of more affordable, safe, transparent, and user-friendly electronic voting systems. Ethereum and its network are among the best because of their consistency, popularity, and availability of smart contracts logic.

### **3. EXISTING SYSTEM**

Elections may be a significant event in a modern democracy, but a key worry for the democracy is that large segments of the global public lack confidence in their electoral process. Even the biggest democracies in the world, such as the United States, Japan, and the Republic of India, nonetheless have flawed legal systems. The main issues with the existing electoral system include booth capturing, election manipulation, vote rigging, and hacking of the electronic voting machine (EVM). We seek to address the concerns with election vote systems in this system by working on them squarely and putting up the E-voting model as a potential solution. A number of well-known block chain frameworks that offer block chain as a service and an electronic Evoting system based on block chain that addresses all limitations can be highlighted by the system. It also preserves participant anonymity while allowing for open scrutiny.

### **4. PROPOSED SYSTEM**

Within a permissioned block chain architecture, the suggested block chain-based electronic voting system incorporates SHA-256 for strong data integrity. It uses smart contracts to control voter eligibility, safe vote encryption, and results tabulation. It consists of separate nodes for voters, election authorities, and validators. SHA-256 cryptographic hashing of votes, strong identity verification techniques, and digital interfaces all contribute to the voting process's security. The block chain's transparency and immutability increase the system's overall trustworthiness, and consensus mechanisms like Proof of Stake guarantee the validation of transactions. Regular security audits are carried out to find and address potential weaknesses, and security measures include encryption for data protection, double-voting prevention, and a secure key management system.

## 5. MODULES DESCRIPTION

### 5.1 ELECTION MANAGER

By entering the address, which is a unique key produced in the ganache framework, the authorised voter can view the contract address that is used for the authorised voter address. Election manager, the private key. Our truly ground breaking, open-source, end-to-end verifiable block chain voting programme. The steps involved in using our block chain voting system to cast a ballot in an election are shown in detail in the infographic below. Subsequently, the voter would furnish the requisite identity details to enable their identity to be authenticated by an Identity Verifier, who would be authorised by the body organising the election beforehand. The voter can make a request there after their identity has been confirmed, and the Registrar will then offer them the appropriate ballot type. After that, the voter would fill out their ballot and safely deposit it into the block chain-based box.

### 5.2 CANDIDATES LIST

The list of candidates that can be voted for includes information on their private keys, gas prices, and gas limits. Using applications built on block chain, a peer-to-peer technology that uses encryption and a write-once, append-many electronic ledger to provide private and secure registration information, has been one way to enable block chain voting.

### 5.3 AUTHORIZE VOTER

The authorised voter has the wallet address's authorization ID, which is unique to that individual, along with important information about the contract address, the price of petrol and the individual's limit that are used to assign votes. A block chain system lowers the need for middlemen, provides transparency, decentralisation, irreversibility, and other important features for an electoral process. The list of candidates that the viewer can view was generated specifically for the simulation. A vital stage in processing data from one end to the other is the exchange of data from electronic voting devices to the nodes. In order to achieve a better outcome than the earlier models, the voting step method uses a block chain based SHA 256 algorithm.

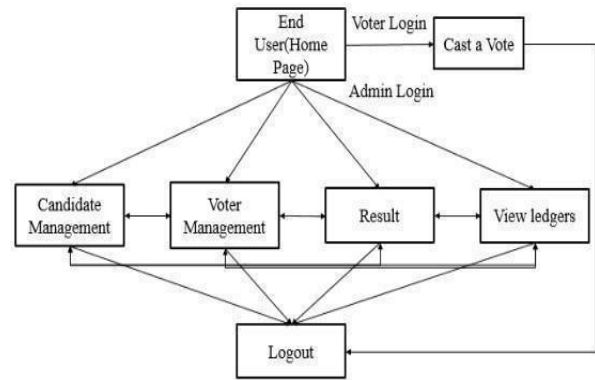
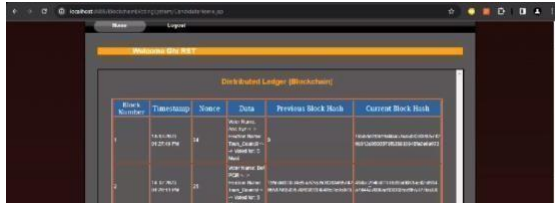


Figure 1 SYSTEM ARCHITECTURE

### 5.4 CONCLUSION

In summary, a safe SHA-256 cryptographic hash function strengthens the proposed block chain-based electronic voting system, which is a potential development in electoral technology. Block chain integration offers benefits including enhanced data integrity, decentralised trust, and simplified efficiency through smart contracts, all of which contribute to a safe, transparent, and unchangeable voting process. This solution solves important issues with conventional voting procedures by potentially improving accessibility, lowering fraud, and offering a verifiable audit trail. However, for implementation to be successful, continual security measures, careful consideration of legal, social, and political concerns, and cooperative efforts to foster public confidence are all necessary.





6.

6.

## SCREENSHOT

- 1 A. Russo, A. F. Anta, M. I. G. Vasco, and S. P. Romano, "Chirotonia: A Scalable and Secure e- Voting Framework based on Blockchains and Linkable Ring Signatures," in *Proc. IEEE Int. Conf. Blockchain*, Melbourne, Australia, Dec. 2021, pp. 417–424.
- 2 W.-J. Lai and J.-L. Wu, "An Efficient and Effective Decentralized Anonymous Voting System," *arXiv preprint arXiv:1804.06674*, 2018.
- 3 F. S. Hardwick, A. Gioulis, R. N. Akram, and K. Markantonakis, "E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy," *arXiv preprint arXiv:1805.10258*, 2018.
- 4 C. Onur and A. Yurdakul, "ElectAnon: A Blockchain-Based, Anonymous, Robust and Scalable Ranked-Choice Voting Protocol," *arXiv preprint arXiv:2204.00057*, 2022.
- 5 R. Fatih, S. Arezki, and T. Gadi, "A Review of Blockchain-Based E-Voting Systems: Comparative Analysis and Findings," *Int. J. Interact. Mobile Technol.*, vol. 17, no. 23, pp. 49–67, Dec. 2023.
- 6 Y. W. Syaifudin et al., "Blockchain-Based E-Voting System: A Decentralized Approach on the Ethereum Private Network," *Int. J. Frontier Technol. Eng.*, vol. 3, no. 1, 2023.
- 7 M. Yan, J. Wang, C. Ai, and M. Han, "An efficient framework for social event invitations that utilises smart device history data," *unpublished manuscript/project report*, [Online]. Available upon request.
- 8 M. Han, M. Yan, J. Li, S. Ji, and Y. Li, "Generating uncertain networks based on historical network snapshots," in *Proc.Int.Computing and Combinatorics*

*Conf.*, Springer, Berlin, Heidelberg, 2021, pp. 747–758.

- 9 S. Ji, Z. Cai, M. Han, and R. Beyah, "Whitespace assessment and virtual backbone construction for cognitive radio networks: From the social perspective," in *Proc. IEEE SECON (Sensing, Communication, and Networking)*, [Year not specified].
- 10 C. Pommier, "The functioning of the private and public key pair," *Symantec Blogs*, 2020. [Online]. Available: <https://www.symantec.com/connect/blogs/how-private-and-public-key-pairworks>
- 11 N. H. R., G. P. M. S., and S. B. G., "E-Voting System Using Blockchain Technology," in *Proc. 2022 4th Int. Conf. on Advances in Computing, Communication Control and Networking (ICAC3N)*, 2022.
- 12 C. Onur and A. Yurdakul, "ElectAnon: A Blockchain-Based, Anonymous, Robust and Scalable Ranked-Choice Voting Protocol," *arXiv preprint arXiv:2204.00057*, 2022.
- 13 A. Kiayias and M. Young, "Robust Verifiable, Non-Interactive Zero Sharing: A Plug-in Utility for Enhanced Voters' Privacy," in *Secure Electronic Voting*, D. A. Gritzalis, Ed. Springer, 2003, pp. 139–152.
- 14 J. Calandrino et al., "Source Code Review of the Diebold Voting System," University of California, Berkeley, 2007. [Online]. Available: <https://votingsystems.cdn.sos.ca.gov/oversight/ttbr/diebold-source-public-jul29.pdfWikipedia>
- 15 S. Mishra et al., "Anonymous Voting Scheme Using Quantum Assisted Blockchain," *arXiv preprint arXiv:2206.03182*, 2022.