Online Voting System Using Block Chain

M. Indrasena Reddy[1*], B. Sowjanya[1], M. Mounika[1], D. Mahima[1]

[1] Computer Science and Engineering, BVRIT Hyderabad College of Engineering for Women, Hyderabad, India
indrasenareddy.m@bvrithyderabad.edu.in

Abstract. Energizing prospects emerge with the execution of block chain innovation into the universe of internet casting a ballot. Considering past contentions encompassing the security and realness of Electronic Democratic Machines (EVMs), this study tries to look at the commonsense benefits of integrating block chain into the democratic interaction. Through the decentralized and unalterable properties of block chain, the proposed E-casting a ballot framework endeavors to make a straightforward and dependable stage for directing decisions. By successfully copying and scattering exchange records across an organization of PCs, block chain innovation ensures the respectability of casting ballot information and safeguards it from any expected altering or control. This paper plans to give a top to bottom investigation of the specialized parts associated with coordinating block chain into E-casting ballot frameworks, including pertinent difficulties and significant variables that should be addressed to accomplish ideal outcomes. Eventually, the reception of block chain-based web based casting a ballot has the capacity to change the electing system, lessen occasions of extortion, and lift resident commitment to a majority rule government.

Keywords: Block chain technology, online voting system, EVMs, Trustworthiness, Fraud prevention, security, Front-end interface, Back-end system, Django, Cryptography.

1. Introduction

Block chain innovation, at first intended for digital currencies like Bit coin, has developed into a unique advantage across enterprises because of its unrivaled security and straightforwardness. This paper investigates its true capacity in improving web-based casting a ballot framework, meaning to address difficulties in customary electing processes. Customary electronic democratic techniques, including Electronic Democratic Machines (EVMs), are vulnerable to control, subverting the validity of political decision results.

Block chain-based voting systems offer a decentralized ledger that ensures tamper-proof and transparent recording of votes. This decentralized nature, combined with advanced cryptographic protocols, safeguards voter privacy and authenticity. Despite

B. S. Babu et al. (eds.), *Proceedings of International Conference on Advanced Materials, Manufacturing and Sustainable Development (ICAMMSD-2024)*, Advances in Engineering Research 257,
https://doi.org/10.2991/978-94-6463-662-8_67

block chain's rise since the 1980s, its significance surged with Bit coin's introduction in 2009. Block chain-powered frameworks stand out for their decentralized consensus processes and immutable record-keeping, overcoming the shortcomings of centralized data systems. However, administrative hurdles and technological readiness remain challenges. Our proposed solution integrates block chain into online voting systems, ensuring the integrity, security, and transparency of every vote. Through decentralized networks, votes are securely registered and remain immutable, supporting electoral integrity. By decentralizing infrastructure, vulnerabilities to cyber threats are minimized, fostering trust and inclusivity in democratic participation. Overall, block chain development promises to revolutionize electronic voting systems by addressing the limitations of traditional methods. Its decentralized and immutable nature ensures the integrity, security, and transparency of electoral processes, enhancing trust in democracy. Ongoing evaluation and refinement are crucial for successful adoption and widespread democratic impact. Foundation, weaknesses to digital dangers are limited, cultivating trust and inclusivity in equitable cooperation. In light of everything, block chain improvement holds guarantee in upsetting electronic projecting a surveying structure, keeping an absence of eye on standard techniques. Its decentralized and never-ending nature guarantees the goodness, security, and straightforwardness of discretionary cycles, redesigning trust in a larger overseas system. Gone on with evaluation and refinement are urgent for specific social occasions and basic reputation based influence.

2. Literature Survey

The mix of IoT and block chain innovation in the democratic cycle to address difficulties related with conventional strategies. It proposes a safe electronic democratic framework that upgrades validity and dependability through components like confirming citizen information with legislative records, producing OTPs and ODPs for added security, and utilizing unique mark biometric confirmation. Every vote is stored on the Ethereum block chain so that there is a permanent and accurate record. Awesome blueprints formalize the process and keep it honest and open. The network aims at addressing current problems in traditional, centralized systems by providing a better model that adds more security, trust, and transparency into the whole process. [1]

It presents a secure internet voting system using Ethereum block chain technology as a remedy to traditional voting problems such as lack of transparency, security threats, and low election turnout. Some of the outstanding attributes of this system include application of smart contracts, hashing as well as encryption for securing anonymous votes; and voter authentication through aadhar numbers and OTPs. The use of private block chain networks restricts access to the voting process to authorized participants only. The paper explicates the relationship between the front-end of an app and backend operations in a block chain thus developing sound architectural base for transparent, secured, user friendly e-voting platform. This system is meant to increase voter turnout and enhance election integrity thus underscoring how block chain can be applied in important applications such as voting. [2]

It provides a comprehensive review of the Secure Digital Voting System based on block chain technology using Multichain to make e-voting secure, transparent, and tamper-proof. The system proposed is designed in layer's format with each layer having its specific purpose to ensure that it has robust and systematic structure. For example, user authentication and vote casting are done through the block chain which allows end-to-end verifiability while maintaining voter anonymity. The model should be simple enough for non-experts and includes a backend database for effective data management. This study demonstrates how block chain can be used in digital voting to address issues of privacy, eligibility and transparency as well as safeguarding democratic processes in the digital age. [3]

It is about how a Secure Electronic Voting System can be implemented using Block chain Technology and the importance of secure and transparent voting. The plan has two separate block chain systems: one for voter details and another for vote details to make it more secure and unbreakable. There are several steps involved such as registration, two-step verification, and each vote being considered a block chain transaction that would guarantee voters' trust as well as transparency. The system uses the SHA-256algorithm for data encryption hence making data integrity and confidentiality possible. An Android app facilitates voter participation whereas voter verification mechanisms allow individuals to validate their votes. By its design, this new method of block chain application highlights security problem solving in e-voting issues while promoting democracy at large. [4]

This paper introduces a decentralized voting scheme with the help of an advanced PHANTOM protocol on a multi-tier distributed ledger system to increase vote security, accuracy and authenticity. This brings in fingerprint authentication and provides polling booths to verify the voters as well prevent malware attacks. The system uses the Borda count method to count votes which eliminates problems like booth capturing and voter threats. The proposed system is not familiar to people as they cannot vote using their mobile apps or web browsers, which reduces its accessibility improvements in terms of usability and security due to the faster and safer voting process that supports a more high-consensus over a larger group (such as rural where lack of literacy) and tries to solve problems concerning hacking EVM & election manipulation by anyone. [5]

The paper proposes the use of a block chain centered e-voting system to alleviate the existing issues in traditional voting systems: security, transparency and voter participation. The shit is coded to be stored on a block chain, so your vote can never be changed and the public at large will always know that you voted. The design of the system ensures the anonymity and integrity of voting data using cryptographic models, as well as providing access to more voters (which can influence voter participation). The process is multi-stage, spanning voter registration, ballot publication, casting votes anonymously and confirming election results on-public register block chain. Security, transparency and cost savings are promised by this system but there are practical challenges related with technical complexity, scale up ability voter education

and legal hurdles. The paper emphasizes the need for more research to reap the benefits of block chain-powered voting [6].

Election Block — the new era of secure and transparent electronic voting on block chain-based IOST ecosystem with fingerprint authentication. The system is developed on a private block chain, thereby providing tamper-proof record of votes helping to enhance traceability and trust. This allows the safe use of fingerprint authentication, thereby reducing the potential for impersonation and providing more security than regular password logins. In its conclusion, the paper also notes that many concerns remain about the centralization of the network and risks around manipulation, with considerations for equitable access remaining significant issues alongside technical complexity. It also provides some human requirements to how these problems could potentially be overcome and the way forward for further exploration as well as development to achieve more wide-scale availability and participation which would otherwise prove rather impractical solutions in this time [7].

3. Model

The role of block chain, Django and MySQL database integration in security transparency and efficiency is the focus of my proposed admission processing system for educational institutions. Django is a powerful web framework that is used to develop both frontend and backend parts of a system. It uses an MVT (Model-View-Template) architecture. The web application adapts better to explain its built-in security features, which make it a user-friendly and secure platform. MySQL database serves as a relational database management system, it stores non-block chain data and provides scalability, performance plus support for ACID properties.

Transaction processing and confirmations are executed internally by the Django application. Smart contracts automate many manual admission procedures, ensuring integrity. They are based on privacy principles: data encryption, access control, surveillance, and compliance with personal data legislation. These measures protect the confidentiality of sensitive admission information stored in both the MySQL database and blockchain technology

4. Experimental Design

Admin adds all the valid voters Aadhar numbers to the database. While registration, users have to enter their Aadhar number, phone number, age. If an Aadhar number is valid i.e., in the database and above 18 years, the user will be registered. After successful registration, the user gets OTP to the phone number. User has to enter that OTP, create a password. If this step is successful, a passphrase will be generated which will be used for further authentication. When voting is enabled, voters have to login using username and password. After that the passphrase has to be entered at the corresponding candidate and has to vote. Ballot will be sealed with a digital signature.

There will be a unique ID generated to view their votes after the results phase is enabled. The person having more number of votes will be displayed in green color.

4.1. Block chain Integration

4.1.1. Models

In Django, models define the structure of database tables. Create a model in the models.py file.

Sample code:

```
from django.db import models
from uuid import uuid4
from datetime import datetime
class VoterList(models.Model):
   username = models.CharField(max_length=30, primary_key=True)
   ph_country_code = models.CharField(max_length=2, default='91'
phone_number = models.CharField(max_length=20, default = '0000000000')
   otp = models.IntegerField(default=0)
   def __str__(self):
      return self.username
```

4.1.2. Forms

Forms handle user input and validation. Create a form class in the forms.py file associated with the model.

Sample code:

```
from django import forms
from .models import User
class UserForm(forms.ModelForm):
       class Meta:
              model = User
              fields = ['username', 'Phone number', 'age']
```

4.1.3. Views

Views process user requests, interact with models and forms, and render templates.

Sample code:

```
from django.shortcuts import render, redirect
from .models import User
from .forms import UserForm
def registration_view(request):
```

```
    if request.method == 'POST':
        form = UserForm(request.POST)
        if form.is_valid():
            form.save()
            return redirect('success_page')  # Adjust the redirect URL
    else:
        form = UserForm()
    return render(request, 'registration.html', {'form': form})
```

4.1.4. Templates

Templates (HTML files) render views and display data.

Sample code:

```
{% extends 'base.html' %}
{% block content %}
  <div class="container">
    <div class="form-container">
      <h2>Registration</h2>
      <form method="post">
        {% csrf_token %}
        {{ form.as_p }}
        <button type="submit">Register</button>
      </form>
    </div>
  </div>
{% endblock %}
```

4.1.5. URLs:

Define URLs in the urls.py file to map views to specific URLs.

Sample code:

```
from django.urls import path
from .views import registration_view

urlpatterns = [
    path('register/', registration_view, name='registration_view'),
    # Add more URL patterns as needed
]
```

4.2. Security Protocols Implementation

Ensuring the integrity and security of the online voting system is paramount. Security protocols feature the use of encryption methods and safe channels for communication to protect the information of users from access without authority. The system is tested to the optimum level possible to find out and rectify potential vulnerabilities. Used here in creating the blocks is the security algorithm known as SHA-256.

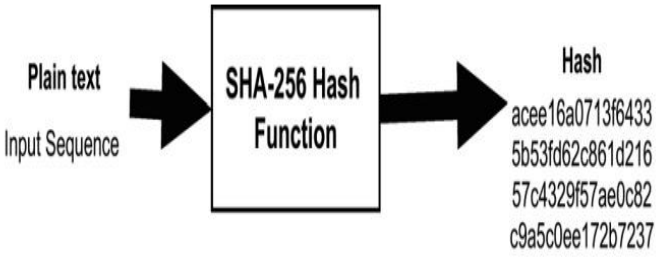

Fig.1. Basic Function of the SHA-256 Hash

SHA-256, a part of the SHA-2 (Secure Hash Algorithm 2) family, has served as the cornerstone in the area of cryptographic hash functions, ensuring that the integrity and security of data are met in a digital era. SHA-256 is from the SHA-2 family, which enjoys cryptographic strength due to the output size of 256-bit. It offers a number beyond astronomical possibilities of all possible hash values that makes it computationally infeasible to reverse-engineer or find collisions, thus leading to different inputs producing the same hash. In essence, cryptographic strength offers a hard barrier against numerous types of attacks, whether a preimage attack or collision attack.

As per our project, for every 5 latest transactions(votes) a block is generated. These 5 transactions are considered as leaf nodes. Pair of these leaves are hashed and a node above them is created. If a node does not have a pair, then its value is duplicated. This continues until the merkle root is generated. So when each time the verify votes button is clicked, merkle root will be freshly generated based on the candidate id in the hash and it is validated with the existing one. In this way we can identify if the votes are tampered.

5. Results and Discussion

Implementing an online voting system using blockchain technology has yielded promising results. The system ensures secure, tamper-proof recording of votes, enhancing the integrity of the electoral process. Transparency is heightened, with every vote securely recorded on the blockchain for independent verification. Accessibility is improved, allowing voters to participate from anywhere with internet access. Overall, the implementation has strengthened democracy by fostering trust, transparency, and inclusivity in the electoral process.

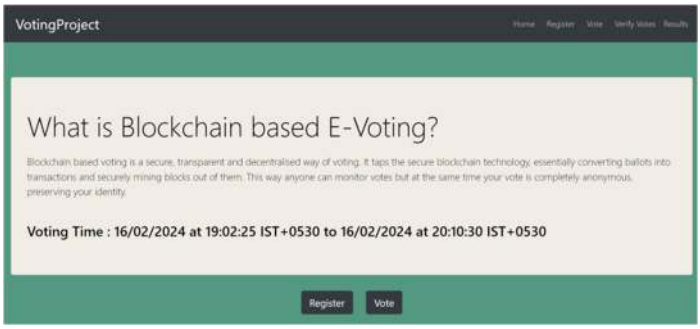

Fig. 2. Home Page

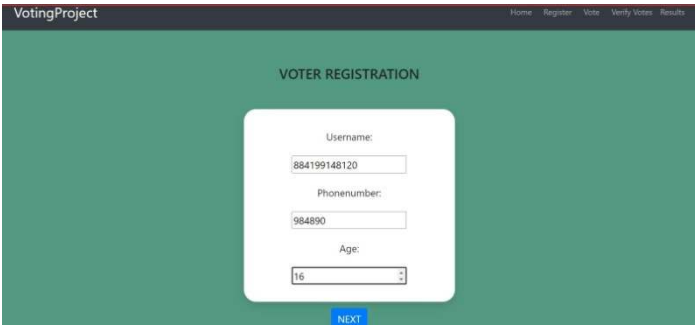

Fig. 3. Registration Page

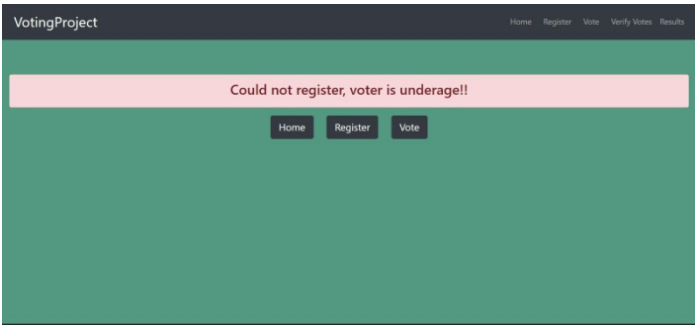

Fig. 4. Invalid Page

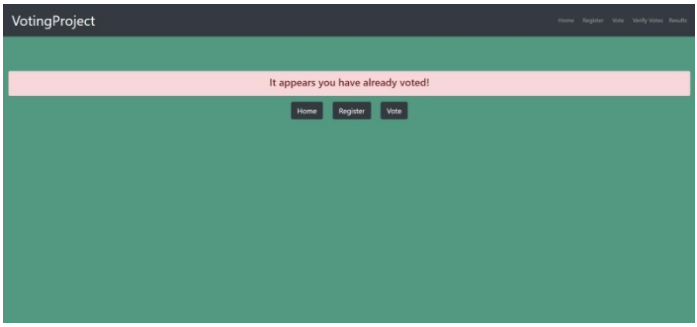

Fig. 5. Checking whether the user casted or not

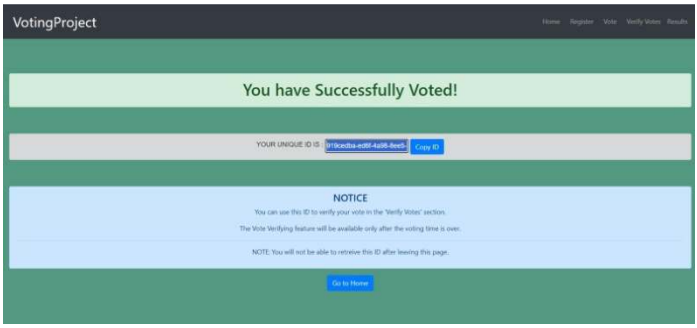

Fig. 6. Successfully Voted

Fig. 7. List of Voters

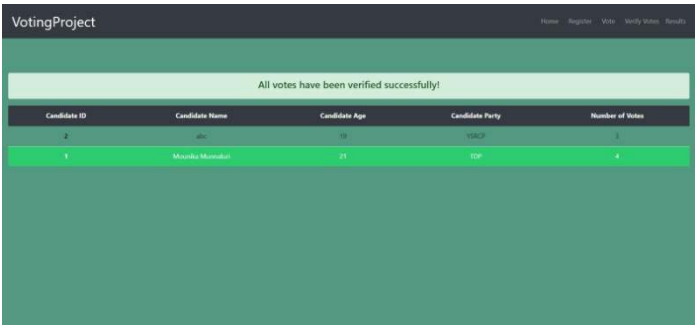

Fig. 8. Result Page

6. Conclusion and Future Scope

This essentially calls for a giant stride into blockchain integration within online voting systems to curb some of the woes of traditional electoral processes. By using the decentralized ledger and advanced cryptographic protocols of blockchain, the proposed solution will ensure every voting procedure is conducted with integrity, security, and transparency. We hope that this will be very helpful in bringing trust and confidence to democratic participation, which is instrumental for enhancing credibility in election results.

The future scope for this project is huge and promising. One area of exploration lies in its adaptation to distinct states, whereby the technology will adapt to meet the particular needs and regulations of the regions. Additionally, this approach enhances cybersecurity to detect and prevent malware attacks on the devices of users. This proactive approach to security ensures that voters can cast their ballots with confidence, free from the threat of digital intrusions. Furthermore, the project may explore better authentication mechanisms, incorporating biometric identification, which would add to the security and ease of the voting process.

References

[1]. A. H. Othman, E. A. A. Muhammed, H. K. M. Mujahid, H. A. A. Muhammed, and M. A. A. Mosleh, "Online voting system based on iot and ethereum blockchain," in 2021 International Conference of Technology, Science and Ad- ministration (ICTSA), pp. 1-6, (2021).

[2]. S. Shukla, A. Thasmiya, D. Shashank, and H. Mamatha, "Online voting applica- tion using ethereum blockchain," in 2018 International Conference on Advances in Computing. Communications and Informatics (ICACCI), pp. 873-880, (2018).

[3]. K. M. Khan, J. Arshad, and M. M. Khan, "Secure digital voting system based on blockchain technology." International Journal of Electronic Government Re- search (IJEGR), vol. 14, no. 1, pp. 53-62, (2018).

[4]. D. D. Kumar, D. Chandini, D. Reddy, D. Bhattacharyya, and T. Kim, "Secure elec-

tronic voting system using blockchain technology," International Journal of Smart Home, vol. 14, no. 2, pp. 31-38, (2020).
[5]. Y. Abuidris, R. Kumar, T. Yang, and J. Onginjo, "Secure large-scale e-voting system based on blockchain contract using a hybrid consensus model combined with sharding," Etri Journalą vol. 43, no. 2, pp. 357-370, (2021).
[6]. B. Ayed, "A conceptual secure blockchain-based electronic voting system," International Journal of Network Security & Its Applications, vol. 9, no. 3, pp. 01-09, (2017).
[7]. M. Ibrahim, K. Ravindran, H. Lee, O. Farooqui, and Q. H. Mahmoud, "Electionblock: An electronic voting system using blockchain and fingerprint authen- tication," in 202) IEEE 18th International Conference on Software Architecture Companion (ICSA-C). IEEE, pp. 123-129, (2021).