A BLOCKCHAIN SOLUTION FOR E-VOTING IN ELECTIONS AT THE UNIVERSITY LEVEL

Devang Sanjay Bhujbal[1],Kajal Chandrashekhar Baviskar[2], Rohan Ramesh Rawate[3],Rohan Anton Pawar[4], Pragati Bhausaheb Chandane[5]

[1] *Student, Department Of Computer Engineering, Adsul's Technical Campus,Ahmednagar,India*
[2] *Student, Department Of Computer Engineering, Adsul's Technical Campus,Ahmednagar,India*
[3]*Student, Department Of Computer Engineering, Adsul's Technical Campus,Ahmednagar,India*
[4] *Student, Department Of Computer Engineering, Adsul's Technical Campus,Ahmednagar,India*
[5] *Guide, Department Of Computer Engineering, Adsul's Technical Campus,Ahmednagar,India*

ABSTRACT

This study was conducted to explore how popular elections are conducted in Kenya and explore some of the challenges that come with it. The study found that blockchain-based e-voting system proved to be a good voting platform to overcome some of the issues currently faced during the voting process. The most common challenges included debates on the reliability of citizens' decisions and decisions, lack of simplicity, ensuring secure data transfer from one hub to another, etc. The customized model was built using JAVA programming language across various performance strategies (SOA, web performance, API) and trialed with Junit and prepared APIs. Blockchain was shown to be highly capable in terms of enabling information security and confidentiality during voting. Hence, Kenya as a nation is likely to benefit from blockchain technology innovations to integrate electronic voter information. This could go a long way in improving not only how Kenyans vote, but also the cost and time spent voting and counting votes. Additionally, it may eliminate contradictions that cause doubts during decision-making.

Keyword :- *Blockchain*

1. INTRODUCTION

Over the past two decades, the emergence and expansion of the Internet has changed the way we live, communicate, and share data. This change is also having an impact on legislative issues, and we are seeing developing countries introduce promising digital voting initiatives aimed at improving election-based systems for their citizens. Advance voting has been around for several years but is still slowly being adopted by decision-making bodies around the world. In Kenya, we have taken many decisions over time, but one of the biggest challenges that discretionary institutions have faced, especially since the controversial declaration of multipartyism, is that they are Is it from the side or is it recognized as legitimate? Required. In 2007, after the presidential election was announced, the country suffered badly. The ensuing massive destruction left approximately 1,300 people dead and more than 600,000 displaced. Large-scale property damage also occurred. The Commonwealth Spectator Group's research report on the 2007 Kenyan elections concluded that ``the Kenya Electoral Commission may have been unable to judge the quality of election administration, which raises questions about the legitimacy of electoral laws." (Kenya Human Rights Commission, 2007). The 2013 election campaign featured voter fundraising presentations via electronic systems. This confirms biometrically that the management of results and voting at the national level is still characterized by the need for consistency, which still contributes to atrocities in various parts. I did. country's . There was a similar draft in a 2018 decision in which the Supreme Court invalidated the race based on the necessity of validity. Our study found that the use of blockchain innovations in the advancement of voting applications provides an opportunity to clarify the issues mentioned, in order to require a single disappointment . Blockchain allows thousands of PCs to work together as a whole, making it more efficient than a few centralized servers. Centralized databases are subject to degradation and typically require third-party assurance to keep the information accurate.

The blockchain's append-only structure ensures that data is added to the database, so to speak, making it difficult to change or delete data in fields that were previously entered.

1.1 Problem Statement

Since the inception of Kenya's multiparty system, many citizens have expressed dissatisfaction, saying they believe elections are not as fair and free as they should be. Since the presidential election, there has been an enormous level of violence in this country. In 2007, for example, approximately 1,300 people were killed, more than 600,000 were displaced, and large-scale destruction of property occurred, particularly in areas where the public believed the candidates had been deceived. In 2013, an appeals court found that judges upheld the government's belief that the elections were free and fair, leading to violence and property destruction in some areas. In 2018, the country had to rerun its presidential elections after the Supreme Court deemed the results unreliable. To ensure free and rational decision-making in our country, we need to reach agreements that guarantee the legitimacy of decisions made. Therefore, this study considers how blockchain innovations can be integrated into voting applications to ensure that the information entered is secure and cannot be changed while moving from point A to point B. To do. The Free Appointments and Boundaries Commission (IEBC) faces legal procurement challenges, particularly in relation to election materials and the Kenya Integrated Decision Management Framework (KIEMS). South Africa-based Pearl Media cited irregularities in the procurement process. Blockchain is a free, open-source system that can be adapted to environments where integrity and privacy are fundamental.

1.2 Objectives

1) Develop and test an electronic voting model that enables the use of valuable data that coexists with the blockchain innovation voting process
2) Expand and highlight the benefits of blockchain electronic voting systems over the currently used IEBC framework. For Ponde

1.3 Scope

The research was conducted with a focus on Kenya's general elections. This section examines the fundamental issues surrounding Kenya's electoral process. The scope of conceptual development of blockchain solutions for electronic voting in university-level decisions includes theoretical systems for using blockchain innovations to facilitate electronic voting (e-voting) specifically tailored to university-level decisions; Includes plans. Here's a breakdown of the major components. Understand the fundamentals of blockchain innovation, its decentralized and persistent nature and potential applications in various fields, counting voting systems. Investigate the challenges and preferences of electronic voting systems compared to traditional paper-based strategies. These include considerations such as security, simplicity, openness, and versatility. Focuses on the unique requirements and characteristics of decision-making in higher education environments. These may include factors such as different partner groups (students, faculty, staff), repeated elections (annual, biannual), and the need for reliable and effective election preparation. Create a comprehensive plan or blueprint for implementing a blockchain-based e-voting agreement specifically tailored to university-level decisions. This includes characterizing the various participants (voters, candidates, directors), designing voting processes, ensuring security and protection measures, and addressing flexibility issues.

2. LITERATURE REVIEW

Blockchain-based Understudy Government Competition Platform Project Writing Research includes a review of existing research, academic studies, case studies, and related works related to blockchain innovation, e-voting frameworks, and their application in educational environments. It is included. A systematic approach to conducting a literature review is as follows.

1. Blockchain innovations in electoral systems: Review academic papers and explore authors discussing the use of blockchain technology in electoral systems, highlighting its benefits, challenges, and potential applications. . See a case study that considers real-world implementations of blockchain-based voting platforms and their consequences.
2. Electronic Voting Framework and Security: Reviews the creation of an electronic voting framework and counts its concepts, security aspects, and vulnerabilities. We feature articles that analyze security risks and attacks on electronic voting systems and suggest measures to mitigate these risks.

3. Decentralized Management and Student Elections: Reviews insightful articles and publications that address the role of student government decisions in education and emphasize the importance of democratic management and student representation. Masu. Here we consider the challenges and opportunities associated with student choice, turnout, candidate selection, and decision-making processes.
4. Blockchain-based voting platform: We study the existing literature on blockchain-based voting phases and their characteristics such as simplicity, durability, and verifiability. Consensus mechanism selection, dedicated contract development, customer interface design.
5. Privacy protection techniques: Review academic papers on privacy protection strategies in electronic voting, zero-knowledge proof counting, homomorphic encryption, and encryption protocols. Adequacy of ensuring voter security while ensuring auditability.
6. Administrative and legal framework: Gather legal and administrative records related to decision-making at the institution, including information security laws, discretionary controls and organizational policies. Read an insightful article that analyzes legitimate proposals for implementing blockchain-based voting phases in educational environments and discusses compliance requirements.
7. Case Study Considerations and Best Practices: Explore case study considerations and best practices from universities and organizations that have successfully implemented blockchain-based voting systems and conducted large-scale electronic elections. Extract nuggets of knowledge from real-world encounters to support undergraduate race-stage planning and development.

3. PROPOSED ARCHITECTURE

The proposed method emphasizes four basic requirements as shown below.
Authentication - Registered people can vote, so to speak. Our framework does not support registration preparation. Registration typically requires certain information and record verification to comply with reporting requirements, which may not be accomplished securely online. Therefore, a co-conspirator must be able to verify the voter's character against an already verified database and allow the voter to vote only once. Anonymity – There should be no interface between the voter's persona and the ballot paper. Accuracy - No votes Must be copyable or deletable and accurate. Venerable - Votes must be irrefutable or accurately counted back to the voter, and the candidate's name serves as the first square on each ballot. Unlike other operations, the premise includes the candidate's title, so to speak. Every time an exchange is registered through a vote, the blockchain is revised. The blockchain will store the data of previous voters who counted the title and their nationally recognizable certification number. If any part loses power at some point, it's easy to find because all parts are connected. The compromise in this case would be to extend or subtract the square. Blockchain is decentralized. So there is nothing to be disappointed about. Blockchain is the realm of real voting. The customer's voice is sent to her one of the hubs within the framework, at which point the hub forwards the voice to the blockchain. Each virtual polling station has a hub in the voting framework, ensuring that the framework is decentralized. Customers must register with their local resident ID number, precinct number, and voter verification information provided to registered voters by a local professional. Customers can vote if it is substantive. Voters must vote for one of the candidates or use their vote to express their opposition to the current policy framework or discretionary decisions. When a user votes, the framework provides a string containing the voter's national identification number, the voter's title, and a hash of the previous vote. Encrypted information is entered in the header of each vote. The data associated with each vote is encrypted using SHA Work, which performs a one-way hash with no known correct reversal.

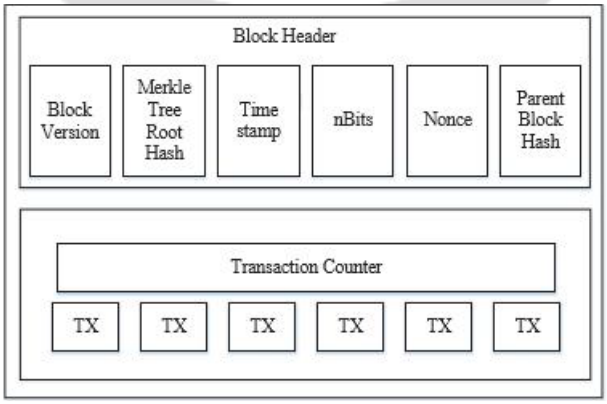

Fig 1-:Blockchain structure

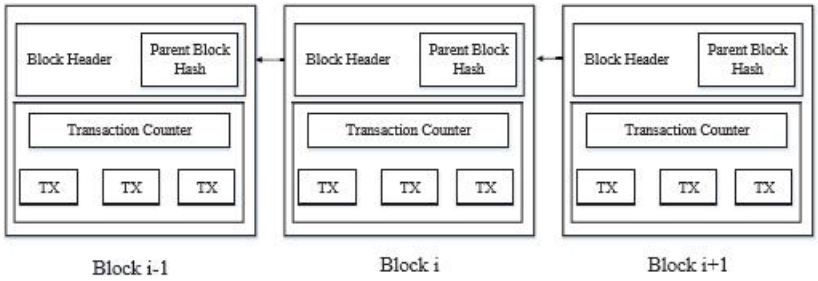

Fig 2-:A blockChain Architecture

OWASP API Security Project: This expansion plan is designed to address the growing number of companies offering potentially insecure APIs as part of their computer software products. These APIs are primarily for internal functionality and third-party interference. Unfortunately, many APIs do not undergo rigorous security testing to protect against hackers. OWASP API Security Extend is intended to help computer software developers and security auditors identify the potential risks of dangerous APIs and explain how to avoid these risks. The OWASP API Security Project creates and maintains an API security risk report and documentation repository for best practices in configuring or evaluating APIs to achieve this goal. OWASP API Security Project Reports are generally free to use.

Categories of security issues covered by OWASP: Authentication and Session Management: Application functionality related to authentication and session management may not always work correctly, allowing an attacker to compromise passwords, keys, or session tokens, or It is possible to impersonate the user by exploiting the execution error. Injections: Injection errors such as SQL, QS, and LDAP injections occur when untrusted data is sent to the translator as part of a command or request. Malicious data from an attacker could allow the translator to execute unintended commands or access data without sufficient authorization. Cross-site scripting occurs when an application selects untrusted data and sends it to a web browser without sufficient permission. This type of attack allows an attacker to run scripts on the victim's browser, hijack the client session, make a website the default, or redirect the client to a compromised location. Masu. Improving security requires reliable setup and execution definitions, especially for applications, systems, application servers and Internet servers, database servers and platforms. Presentation of sensitive data through web applications where sensitive data such as credit cards, payment IDs, and verification credentials are not adequately protected. For some time now, web applications have had no control over the behavioral level of access, and this is evident in the client interface, so the benefits of access must be considered at a functional level. If an application is not validated, an attacker can create it and gain functionality without sufficient consent.

Conceptual Model: As shown in Figure 3, the customer must log in using the username and password given to the registered voter by the local expert (IEBC). If the volume is large, customers should have the right to vote. Voters must vote for one candidate for each office. When a user submits a vote, the tool creates a string containing the voter's title and a hash of the previous vote. The encrypted information is entered into the square header of each survey submitted. The information associated with each ballot is encrypted using a one-way hash function of SHA with no known reversal. The table below references the Show e-voting framework and was

.

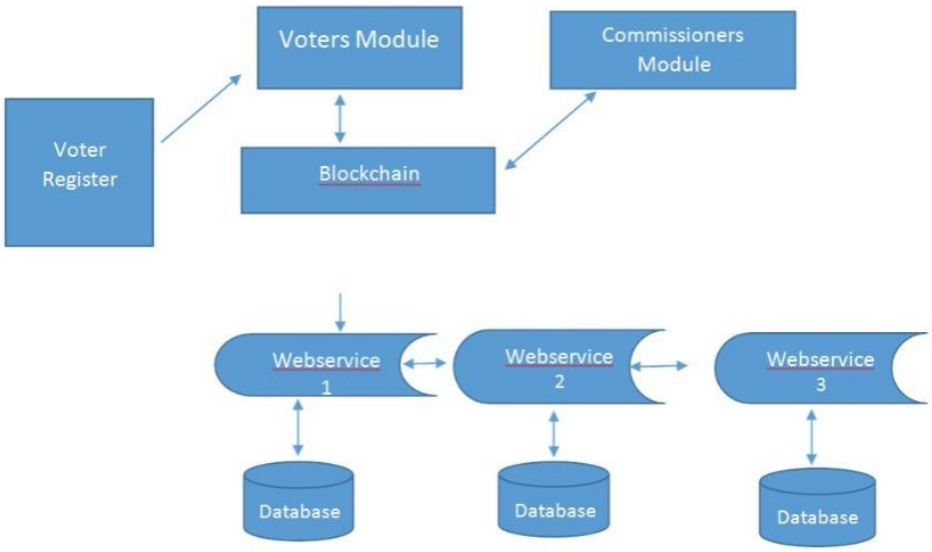

Fig 3-:E-voting system model

4.METHODOLOGY

This area tracks the proposed rapid application development strategy, collecting information on plans, data sources, data collection information, methods and strategies, and system design. The model was built using the RAD (Quick Application Advancement) concept. RA is a development cycle that aims to make the further development of the framework much faster and of higher quality compared to traditional life cycles. RAD emphasizes rapid and iterative release of models and applications, and primarily uses object-oriented programming techniques that inherently promote software reuse. In the initial phase, we first conducted a research tour to explore the real problems facing the target customers. In this case, this was done through personal interviews, document reviews, discussions with the target customers, and the creation of audit studies. In the customer planning phase, development was primarily done using the Java programming language. This draft was created taking into account the current problems. In the development phase of the cycle, the model framework was created. Barriers and characteristics to pre-action/mediation were observed and recorded. We've allowed a number of customers to use our framework and summarized their views on it. Finally, common findings were distinguished and the consequences of the activities were clearly identified. Data Collection Tools: This study was a subjective study of strategies used in various fields such as computer science. His goal is to "know" or empathize with the miracle. The specific methods used to examine the strategies used were face-to-face meetings and analysis of life stories and trade analysis surrounding the Kenyan decision. The purpose of this phase was to identify the objectives of the Constitution and Border Freedoms Commission (IEBC), trade objectives, and key implementation guidelines for addressing race-related issues. This stage also formed innovations, applications and personal skills in the current environment. General trading dictionary, trading rules, commercial artists, and key trading usage examples. This phase begins with the creation of "current" and "future" trading models. A systems review, planning and implementation analysis of the current coordination framework that currently exists in Kenya. The review of the situation included examining existing coordination frameworks and identifying bottlenecks in each mode using various information gathering methods. Problem research and needs assessment. Analysis of current processing: Examination of data streams related to vote preparation reveals that a combination of computerized and manual frameworks are currently being used simultaneously, resulting in systems facing the need for judgment and simplicity. It became clear that Moreover, there is no unwavering quality in the results presented, as evidenced by the post-election malice in different parts of the country. Current plans:Preparation begins with voter registration using the Kenya Integrated Electoral Management Framework (KIEMS) units, followed by verification of voters during voting. Voting takes place in manual ballot boxes, with records of the seals kept for each electoral office before being verified. This begins with breaking the seals (in the vicinity of party leaders and observers at the counting stations) and then pouring the substance into counting vessels. A poll is then conducted to determine its legitimacy, which is then classified

according to the support of the candidates. Counting operation and recording of forms 33. Verified ballot papers are bound into bundles of 25, forms 34 or 35 are filled out individually, explaining rejected votes if necessary. This is followed by reporting and transmission to the Voter Census Centre, and finally, manual forms 34, 35 and 36 are sent from the states to the National Counting Centre (NTC). (IEBC, 2016) Analysis of the current framework information: The study found that many of the challenges faced by the flow were due to various forms filled by returning officials, resulting in incorrect tabulation of information, resulting in discrepancies in the results. . Proposed system. This model was planned and created as a proof-of-concept draft that blockchain innovations can definitely be used to conduct races in Kenya without compromising the results. Development tools: The framework was built with MSQL database, Java Advancement Pack, and Java Advancement Pack. NetBeans as a coordinated development environment and Glassfish were created to allow for the development of distributed systems. The goal of a good, reasonably secure data framework is to ensure that data collection is continuous after the fundamentals of data security are in the IT fundamentals, policies, and methodologies. -

1. Integrity - Provision to prevent unauthorized third parties from modifying data in traffic. This is achieved by replicating the database in multiple locations. When making decisions, the focus is usually on the immutability of the votes. Many well-known blockchain stages use Merkle trees (some also use other variants of Merkle trees) to validate decisions about the information contained in the blockchain. If a single piece of information has actually been changed or tampered with, this can be easily detected using Merkle tree confirmation. This property of blockchain, which ensures that votes cannot be changed or altered once they are recorded on the blockchain, helps ensure the permanence of votes and confirmation of verdicts.
2. Authentication - How each module uses a password to verify the identity of the user requesting access.
3. Authorization - A strategy for establishing customer rights and interests during interaction with a system.
4. Confidentiality – This means, so to speak, ensuring that all sensitive information transmitted can be read by authorized parties.

5. RESULTS

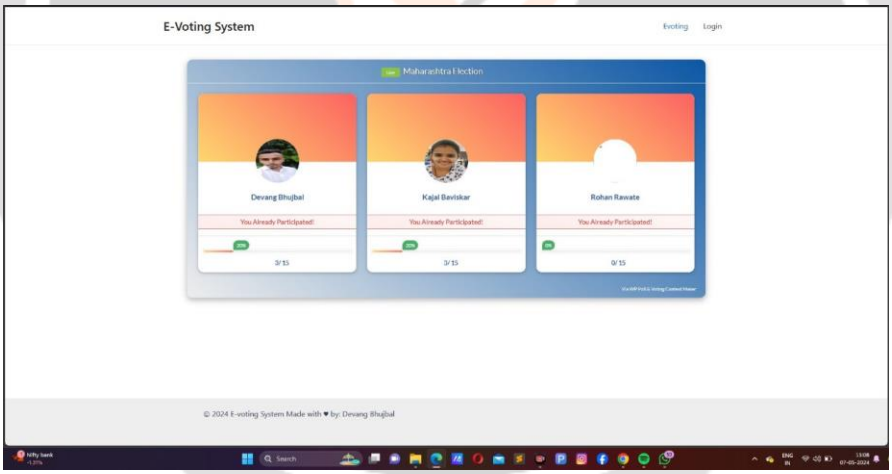

Fig: Front page

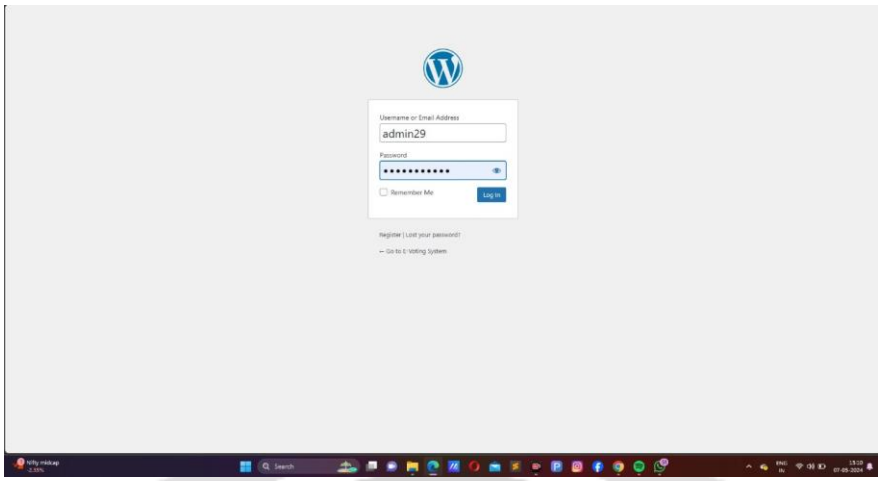

Fig: Login Page

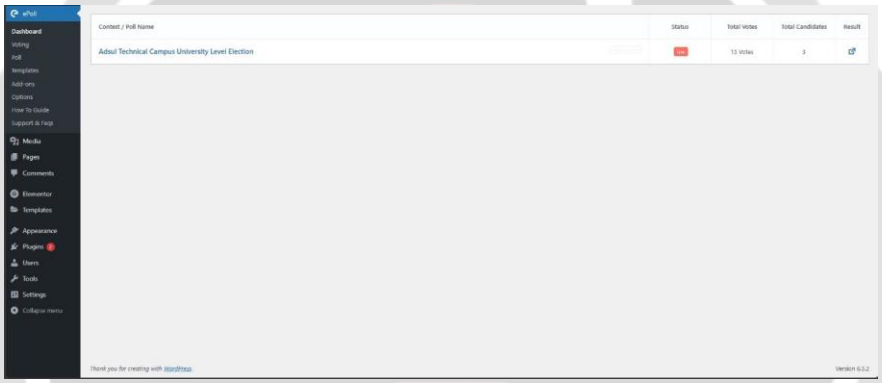

Fig: Dashboard

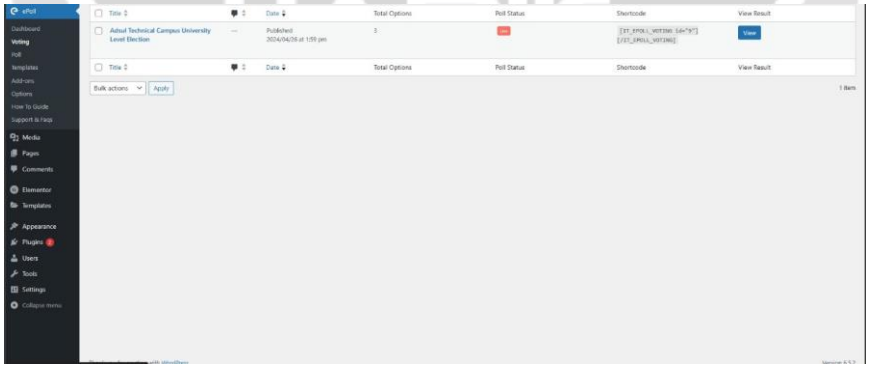

Fig: Voting contest

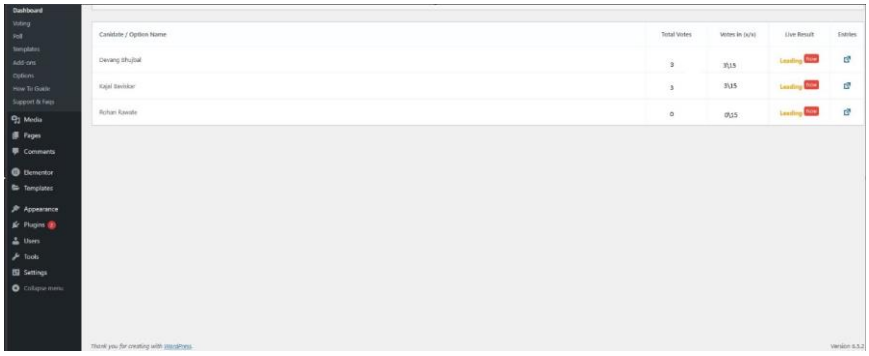

Fig: Dashboard result

6. CONCLUSIONS

In conclusion, implementing blockchain-based systems for electronic voting in university elections offers significant benefits in terms of reliability, simplicity, efficiency, and security. By leveraging blockchain innovation, universities can streamline election preparation, increase student availability, reduce regulatory costs, and reduce the risk of extortion and manipulation. The immutable nature of blockchain ensures efficiency in election preparation, making it extremely problematic for malicious actors to modify or alter the voting process. Furthermore, the simplicity and verifiability of blockchain gives partners confidence in the validity and accuracy of decision outcomes. Looking ahead, the future scope of blockchain-based electronic voting in university-level elections is promising. As innovation advances and management systems emerge, blockchain systems will become more versatile and flexible, allowing them to work with existing higher education systems. In any case, to realize the full potential of blockchain-based electronic voting in higher education decision-making, it is important to address challenges such as administrative compliance, innovation boundaries, and barriers to appropriation.

7. FUTURE SCOPE

Conceptual development of blockchain systems for electronic voting in university election campaigns typically includes several key components. Blockchain system: A distributed arrangement of hubs that maintains a transmission record of all voting exchanges. This ensures the simplicity, durability and security of the voting process. Smart contract: A self-executing contract where the terms and conditions are simply written in code. For electronic voting, smart contracts can monitor the entire voting process, including voter registration numbers, ballot creation, voting, and vote tabulation. Voter Identity Verification: All voters must be verified to ensure they are eligible to vote. This can be done through computerized personas or other verification tools that feed coordinates into the blockchain system. Create Polls: Keen Contracts allows you to create advanced polls that include candidates and choices for your race. These votes will be stored securely on the blockchain and made available to eligible voters. Preparing to vote: Eligible voters can vote securely using cryptography to ensure confidentiality and predict change. Each vote is recorded as an exchange on the blockchain. Vote tally: Blockchain tallies votes by executing smart contract principles. Because blockchain is immutable, the legitimacy of voting results is guaranteed and attempts to change results are easily detected. Auditing and directness: The directness of blockchain allows partners to audit the entire voting phase to ensure its adequacy and completeness. Security Measures: Strict security measures, including encryption, contractual components, and permissions, are in place to prevent unauthorized access, control, or modification of the voting framework.

8. REFERENCES

1. (IFES) Africa International foundation For electoral, 2017. Elections in Kenya. 2017 General Elections.
2. Avison, D. B. R. a. M. M., 2001. "Controlling action research projects".Information Technology & People,14(1), pp. 28-45.

3. Uamakant, B., 2017. A Formation of Cloud Data Sharing With Integrity and User Revocation. International Journal Of Engineering And Computer Science, 6(5), p.12.
4. Butkar, U. (2014). A Fuzzy Filtering Rule Based Median Filter For Artifacts Reduction of Compressed Images.
5. Butkar, M. U. D., & Waghmare, M. J. (2023). Hybrid Serial-Parallel Linkage Based six degrees of freedom Advanced robotic manipulator. Computer Integrated Manufacturing Systems, 29(2), 70-82.
6. Butkar, U. (2016). Review On-Efficient Data Transfer for Mobile devices By Using Ad-Hoc Network. International Journal of Engineering and Computer Science, 5(3).
7. Butkar, M. U. D., & Waghmare, M. J. (2023). Novel Energy Storage Material and Topologies of Computerized Controller. Computer Integrated Manufacturing Systems, 29(2), 83-95.
8. Butkar, U. (2014). Synthesis of some (1-(2, 5-dichlorophenyl)-1H-pyrazol-4yl (2-hydroxyphenyl) methanone and 2-(1-(2, 5-dichlrophenyl)-1H-pyrazol-4yl) benzo (d) oxazole. International Journal of Informative & Futuristic Research (IJIFR), 1(12).
9. Butkar, U. (2014). An execution of intrusion detection system by using generic algorithm.
10. Butkar, M. U. D., & Waghmare, M. J. (2023). Crime Risk Forecasting using Cyber Security and Artificial Intelligent. Computer Integrated Manufacturing Systems, 29(2), 43-57.
11. Butkar, U. D., & Gandhewar, N. (2022). Accident detection and alert system (current location) using global positioning system. Journal of Algebraic Statistics, 13(3), 241-245.
12. Butkar, M. U. D., & Waghmare, M. J. (2023). An Intelligent System Design for Emotion Recognition and Rectification Using Machine Learning. Computer Integrated Manufacturing Systems, 29(2), 32-42.
13. Butkar, M. U. D., & Waghmare, M. J. (2023). Advanced robotic manipulator renewable energy and smart applications. Computer Integrated Manufacturing Systems, 29(2), 19-31.
14. Butkar, M. U. D., Mane, D. P. S., Dr Kumar, P. K., Saxena, D. A., & Salunke, D. M. (2023). Modelling and Simulation of symmetric planar manipulator Using Hybrid Integrated Manufacturing. Computer Integrated Manufacturing Systems, 29(1), 464-476.
15. Butkar, U. D., & Gandhewar, D. N. (2022). ALGORITHM DESIGN FOR ACCIDENT DETECTION USING THE INTERNET OF THINGS AND GPS MODULE. Journal of East China University of Science and Technology, 65(3), 821-831.Baskerville, R. a. M. M., 2004. "Special Issue on Action Research in Information Systems: Making ISResearch Relevant to Practice- Foreword,". MIS Quarterly (28:3), 28(3), pp. 329-335.
16. Baskerville, R. a. P.-H. J., 1999. "Grounded action research: a method for understanding IT in practice,"Accounting, Management and Information Technologies, 9(1), pp. 1-23.
17. Baskerville, R. a. W.-H. A. ". C. P. o. A. R. a. a. M. f. I. S. R., 1996. "A Critical Perspective on Action Research as a Method for Information Systems Research,". Journal of Information Technology, Volume11, pp. 235-246.
18. Baskerville, R. C. o. t. A. (. 1., 1999. "Investigating Information Systems with Action Research,", s.l. AIS E-library.
19. Chaum., D., 2004. Secret-ballot receipts: True voter-verifiable elections..IEEE Security & Privacy, 2(1),pp. 38-47.
20. COMMONWEALTH, S., 2013. Report of the Commonwealth Observer Group. KENYA GENERALELECTIONS.
21. Cybernetica., 2013. “Internet Voting Solution.”. [Online] Available at: https://cyber.ee/uploads/2013/03/cyber_ivoting_NEW2_A4_web.pdf.[Accessed 20October 2018].