

Decentralized Voting System Using Blockchain

RAGHULAN D S¹, AMAL ROY A²

^{1,2}*Department of Information Technology Velammal Engineering College, Chennai, India*

Abstract- The growing reliance on digital systems in governance and institutional decision-making has increased the need for secure, transparent, and trustworthy voting mechanisms. Traditional voting methods used in academic institutions often suffer from issues such as impersonation, vote tampering, manual errors, and lack of transparency. To address these challenges, this paper presents a decentralized voting system built using blockchain technology and enhanced with facial recognition-based authentication. The proposed system ensures voter authenticity by verifying each participant through Face++ cognitive services before allowing vote casting. Votes are encrypted using the SHA-256 algorithm and securely recorded on a blockchain, ensuring immutability, transparency, and resistance to tampering. Ganache is used to simulate the Ethereum blockchain environment, while Node.js manages backend operations and smart contract interactions. The system follows a modular architecture consisting of Student, Candidate, and College Management modules, enabling efficient election management and real-time result monitoring. By combining biometric verification with decentralized ledger technology, the proposed solution eliminates multiple voting, enhances trust in the election process, and provides a reliable digital alternative to conventional paper-based voting systems. This work demonstrates the practical applicability of blockchain-based voting systems in educational institutions and similar controlled environments.

Index Terms- Decentralized Voting System, Blockchain Technology, Facial Recognition Authentication, Smart Contracts, Secure E-Voting, Biometric Verification, Ganache Framework, Node.js Backend, Data Integrity, Transparency and Trust

I. INTRODUCTION

Voting is a fundamental process in any democratic environment, including academic institutions where student elections play a key role in leadership selection and representation. Despite its importance, many colleges still rely on traditional paper-based or semi-digital voting methods that

are prone to impersonation, vote manipulation, lack of transparency, and delayed result processing. These limitations reduce trust in the electoral process and increase administrative overhead.

With the rapid advancement of digital technologies, blockchain has emerged as a reliable solution for building secure and transparent systems due to its decentralized, immutable, and tamper-resistant nature. At the same time, biometric authentication techniques such as facial recognition have proven effective in verifying user identity and preventing unauthorized access. However, most existing voting systems adopt either centralized control or weak authentication mechanisms, leaving critical security gaps unaddressed.

This project proposes a decentralized voting system using blockchain integrated with facial recognition to overcome these challenges. The system leverages smart contracts deployed on a blockchain network to securely record votes, ensuring transparency and immutability throughout the election process. Facial recognition using Face++ cognitive services is employed to authenticate voters, guaranteeing that only eligible users can cast a single valid vote. Ganache is used to simulate the blockchain environment during development, while Node.js manages backend operations and interaction between system components. By combining decentralized storage with biometric verification, the proposed system delivers a secure, reliable, and efficient digital voting platform tailored for academic institutions.

II. PREPARATION OF YOUR PAPER

This paper on a decentralized voting system using blockchain and facial recognition is prepared using Microsoft Word in accordance with Springer's proceedings template. The formatting, structure, and citation style strictly follow Springer guidelines to

ensure uniformity and publication compatibility. All required source files, including the main document, figures, and references, are maintained and submitted along with the final PDF version. References are formatted using Springer-recommended bibliographic styles such as MathPhySci and Basic to ensure accuracy during typesetting and indexing. The volume editors or program chairs serve as the primary point of contact throughout the submission and publication process, assisting with formatting validation and final approval.

1.1 Structuring Your Paper Affiliations and Email Addresses

The author names are listed at the top of the paper, followed immediately by their respective institutional affiliations. For this project, all authors are affiliated with the Department of Information Technology, Velammal Engineering College, Chennai, India. The affiliation includes the institution name, city, and country, which is sufficient for Springer proceedings. Postal codes may be included but are not mandatory. Each author’s email address is provided on a new line directly below the affiliation. The corresponding author is clearly indicated using an envelope symbol, and their email address is mandatory. Including email addresses for all authors is strongly recommended, as Springer uses these details to provide authors with access to their published eBook via the MySpringer platform, along with applicable author benefits.

Headings and Section Organization

All headings in the paper follow Springer’s capitalization rules, where major words such as nouns, verbs, and adjectives begin with capital letters, while articles, conjunctions, and prepositions remain in lowercase. With the exception of the paper title, all headings are aligned to the left.

Only the first two levels of headings are numbered, ensuring a clean and readable structure. The paper avoids the use of a “Section 0” and begins numbering directly from the introduction. This structured hierarchy improves clarity and helps

readers easily navigate through the system design, implementation, and evaluation sections of the project.

The heading levels used in this paper are as follows:

Heading Level	Heading	Font Size and style
Title	Decentralized Voting System Using Blockchain	14 pt, Bold
1st-level heading	1 Introduction	12 pt, Bold
2nd-level heading	2.1 Proposed System	10 pt, Bold
3rd-level heading	Module Description.	10 pt, Bold
4th-level heading	Security Mechanism.	10 pt, Italic

Table captions are always placed above tables, while figure captions are placed below figures, in accordance with Springer formatting standards.

Hyphenated Words in Headings

When hyphenated words appear in headings, capitalization follows Springer’s standard rule: if the first word can stand independently, the second word is capitalized. This rule is consistently applied across all section titles in the paper, particularly in headings related to system architecture and security mechanisms.

Examples of compliant heading styles include:

- A Secure and Transparent Blockchain-Based Voting System
- Facial-Recognition-Based Authentication Framework
- User-Friendly and Extendable Decentralized Architecture

Lemmas, Propositions, and Theorems

If formal definitions such as lemmas, propositions, or theorems are included, they are numbered sequentially starting from Lemma 1, Proposition 1, or Theorem 1, without incorporating section numbers. This paper primarily focuses on system design and implementation; however, any formal statements related to cryptographic validation or

blockchain integrity follow this numbering convention to maintain consistency with Springer guidelines.

2.2 Length of Papers

The proposed project, Decentralized Voting System Using Blockchain with Facial Recognition, is developed as a complete and fully implemented system, making it suitable for submission as a full research paper. Springer proceedings generally accept full papers in the range of 10 to 20 or more pages, where each page contains approximately 300–400 words. This length allows sufficient scope to clearly explain the problem statement, system design, architecture, implementation details, experimental results, and discussion.

Given the involvement of advanced technologies such as blockchain, smart contracts, facial recognition using cognitive services, and decentralized system architecture, a shorter paper would not adequately capture the technical depth and practical contributions of the work. Therefore, a paper length of 10–12 pages, corresponding to approximately 3,500–4,500 words, is considered appropriate for this project. This ensures meaningful scientific content, proper analysis, and clear presentation, while also meeting Springer’s standards for indexing and visibility on SpringerLink.

2.3 Fonts

This paper follows Springer’s formatting requirements to ensure compatibility with full-text XML publication. The manuscript is prepared using the official Springer Word template, which is based on the Times font family. All text elements, including headings, body text, tables, and captions, strictly adhere to the prescribed font style and size defined in the template. Using the recommended font ensures consistency, readability, and smooth processing during typesetting. Manuscripts prepared with fonts other than those specified by Springer may be automatically converted during production to maintain uniformity across the proceedings.

2.4 Page Numbering and Running Heads

Page numbers and running heads are not included in this manuscript, as they will be added by the

publisher during the final typesetting process. If the full title “Decentralized Voting System Using Blockchain with Facial Recognition” is considered too lengthy for use as a running head, it may be shortened to “Blockchain- Based Decentralized Voting System” to ensure clarity and consistency in the published proceedings.

2.5 Figures and Tables

All figures and tables included in this paper are designed to be clear, legible, and consistent with Springer publication standards. System diagrams and architectural representations are created using vector-based graphics to ensure high resolution and clarity during both digital and print rendering. Line drawings maintain uniform thickness, uninterrupted connections, and sufficient spacing to avoid visual clutter. Text labels within figures use font sizes greater than 6 pt to ensure readability.

Figures are numbered sequentially and accompanied by descriptive captions positioned below each figure, while table captions are placed above their respective tables. Each figure and table is explicitly referenced within the text to maintain contextual continuity. Screenshots are included only where necessary and are carefully selected to highlight essential system functionality without unnecessary detail.

In the printed version, figures may appear in grayscale; therefore, all diagrams are designed to remain interpretable in both color and black-and-white formats.

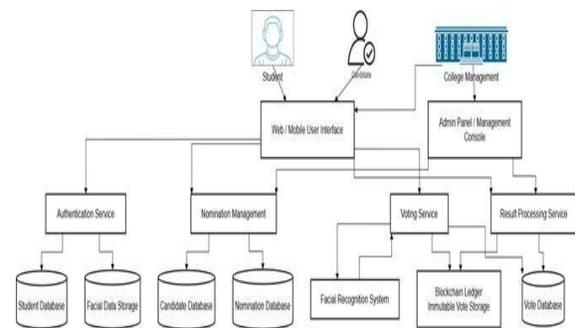


Fig. 1. System Architecture of the Decentralized Voting System Using Blockchain and Facial Recognition

The figure illustrates the overall architecture of the proposed decentralized voting system. It depicts the interaction between students, candidates, and college management through a unified web or mobile interface. The authentication service integrates facial recognition for voter verification, while nomination management and voting services handle candidate validation and vote casting. Votes are securely recorded in an immutable blockchain ledger, and result processing services compute and display election outcomes. Dedicated databases support secure storage of student records, candidate details, nominations, and voting data.

2.6 Formulas

Mathematical expressions used in the proposed decentralized voting system are presented as standalone, centered equations to ensure clarity and ease of reference. Each equation is numbered consecutively using Arabic numerals enclosed in parentheses and aligned to the right margin. These equations are referenced explicitly within the text where required.

For example, cryptographic hash generation used to secure each vote can be represented as:

$$H(v) = \text{SHA256}(v \parallel t \parallel k) \quad (1)$$

where v represents the vote value, t denotes the timestamp, and k is a unique voter identifier. This formulation ensures vote integrity and prevents tampering. Equations are punctuated consistently with the surrounding text, maintaining a small space before any concluding punctuation.

2.7 Footnotes

Footnotes are used sparingly in this paper and only where additional clarification is necessary without interrupting the flow of the main text. Superscript numerals are placed immediately after the relevant word or, when referring to an entire phrase or sentence, following the appropriate punctuation mark.¹

For remarks related to the paper title or author information in the header, symbolic markers are used instead of numeric footnotes. Footnotes are not included within the abstract section, in

accordance with Springer formatting guidelines.

2.8 Program Code

Program code segments related to the implementation of the decentralized voting system are presented in a monospaced typewriter font to clearly distinguish them from descriptive text. Code snippets are included only when they contribute directly to understanding the system logic, such as smart contract execution or backend processing.

An example pseudocode snippet illustrating vote validation and blockchain storage is shown below:

```
function castVote(voterID, candidateID):  
  if verifyFace(voterID) == true:  
    if hasVoted(voterID) == false:  
      voteHash = SHA256(voterID + candidateID +  
        timestamp)  
      storeOnBlockchain(voteHash)  
      markAsVoted(voterID)  
    else:  
      rejectVote()  
  else:  
    denyAccess()
```

This representation demonstrates the integration of facial authentication, vote validation, cryptographic hashing, and immutable blockchain storage within the voting workflow.

2.9 Citations by Number

References in this paper are cited using Arabic numerals enclosed in square brackets and are not superscripted. Citations follow a sequential numbering order based on their first appearance in the text. Multiple references are cited using a hyphenated range or comma-separated list, arranged in ascending numerical order.

Examples include a single citation [3], multiple citations [4–6], and combined references [2, 7]. When an author's name is mentioned directly in the text, the corresponding citation number follows, as in Majumder et al. [1].

All references are listed using the Latin alphabet. Titles originally published in other languages include an appropriate language indicator. Only

works directly relevant to blockchain-based voting, biometric authentication, or secure distributed systems are included. Wherever possible, Digital Object Identifiers (DOIs) are provided to enhance accessibility and cross-referencing within SpringerLink.

2.10 Ethics and Permissions

All figures, tables, and textual content included in this paper are original or appropriately referenced. No copyrighted material has been reproduced without proper permission from the respective rights holders. The authors acknowledge that the manuscript may be subject to plagiarism screening upon submission.

Any detected ethical violations, including plagiarism, may result in retraction and formal notification to the concerned academic authorities. The authors adhere to Springer's publishing ethics and conflict-of-interest guidelines and affirm that the work presented is original and conducted with academic integrity.

2.11 Avoidance of Self-plagiarism

While building upon existing knowledge in blockchain and electronic voting systems, this paper ensures originality in both content and presentation. Any overlap with previously published work by the authors has been minimized and appropriately cited. Where reuse of material is necessary, permission has been obtained from the original publishers when required, maintaining full transparency.

III. ACKNOWLEDGMENTS

The authors would like to express their sincere gratitude to the Department of Information Technology, Velammal Engineering College, for providing the necessary infrastructure and academic support to carry out this project. Special thanks are extended to the project guide for continuous guidance, constructive feedback, and encouragement throughout the development and documentation of this work.

REFERENCES

[1] Majumder, S., Ray, S., Sadhukhan, D.,

Dasgupta, M., Das, A.K., Park, Y.: ECC-EXONUM-eVOTING: A Novel Signature-Based e-Voting Scheme Using Blockchain. *IEEE Trans. Dependable Secure Comput.* 20(4), 3121–3135 (2023).

[2] Chaudhary, S., Shah, S., Kakkar, R., Gupta, R., Alabdullatif, A., Tanwar, S., Sharma, G., Bokoro, P.N.: Blockchain-Based Secure Voting Mechanism Underlying 5G Network: A Smart Contract Approach. *IEEE Access* 12, 45678–45692 (2024).

[3] Almeida, R.L., Baiardi, F., Di Francesco Maesa, D., Ricci, L.: Impact of Decentralization on Electronic Voting Systems: A Systematic Literature Survey. *IEEE Commun. Surv. Tutor.* 25(3), 1890–1912 (2023).

[4] Yi, H.: Securing e-Voting Based on Blockchain in Smart Cities. *Int. J. Inf. Secur.* 21(2), 221–234 (2022).