

PQ-Vote: A Post-Quantum Block chain-based Voting System with AI-driven Security & Analytics

**Gokul G¹, Dr. M Krishnamurthy², Balamurugan P³, Dr Jasmine Paul⁴,
Abiram M J⁵, Ms Aida Jones⁶**

²Professor & HOD,

^{1,2,3,4,5,6}Department of Artificial Intelligence and Data Science

^{1,2,3,4,5,6}KCG COLLEGE OF TECHNOLOGY

Chennai, India

¹22ad14@kcgcollege.com, ²hodads@kcgcollege.com, ³22ad07@kcgcollege.com,

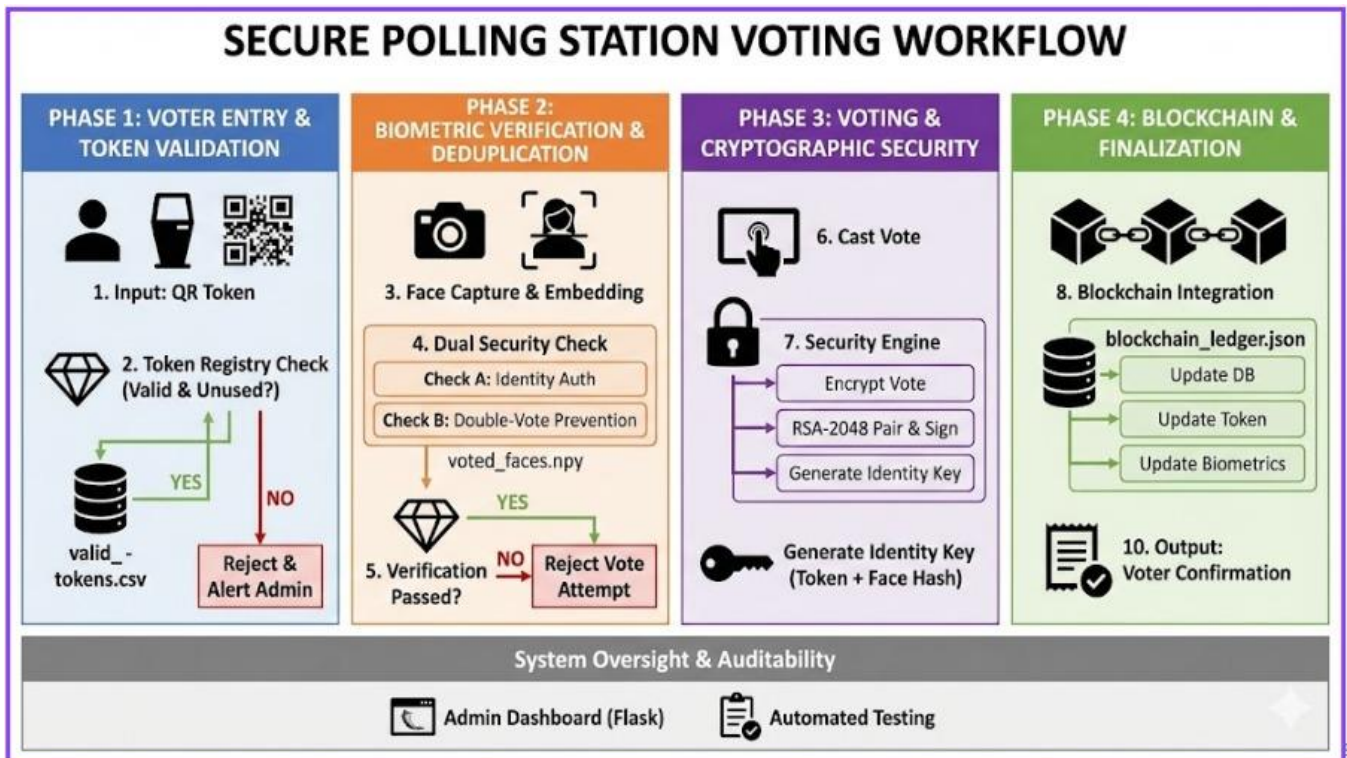
⁴Jasmine.ads@kcgcollege.com, ⁵22ad01@kcgcollege.com, ⁶Aida.ads@kcgcollege.com

Abstract

This project offers a free Python blockchain voting system that combines artificial intelligence with simulated post-quantum cryptography to enhance the security and transparency of the voting process. It operates in a controlled polling station, and the voting process remains as simple as people are accustomed to—it's just a whole lot more secure. Rather than keeping votes in one central location, this system employs a tamper-proof blockchain ledger system, making it much more difficult for anyone to interfere with the vote. Now, regarding the quantum security aspect: since actual quantum computers aren't exactly abundant, this system employs the PyCrypto library to simulate post-quantum cryptography. This way, votes remain encrypted and easily verifiable, even in a simulated setting. The AI components kick in to verify the identities of voters, keep an eye out for anything fishy or suspicious, and monitor the system itself. Essentially, if anyone tries to cheat or something fishy occurs, it detects it immediately. Accessibility is a huge problem in this regard. This voting system is designed to be accessible to everyone, including those who are unable to read or are struggling with technology. The voting system is based on symbols, and there is also audio support available if needed. Furthermore, all of this is done directly on the local computers, with very little interaction with the internet, which is great for privacy and does not cost anything. It has been tested, and it seems that the combination of blockchain technology, AI monitoring, and post-quantum cryptography (even if it is only simulated) makes this voting system more trustworthy and easier to audit than the traditional electronic voting systems. It is good enough to be used for research at this point, and it can be expanded for bigger applications in the future.

1. INTRODUCTION

Elections are the backbone of any democracy, but let's be honest, the voting process is still beset with some serious problems in terms of security, transparency, and public confidence. In India, they have brought in the idea of Electronic Voting Machines (EVMs) with Voter Verifiable Paper Audit Trails (VVPATs), which has certainly made the voting process quicker, but simultaneously, there are concerns



about hacking, too much government interference, and the fact that it is difficult to audit the voting process. And let's not even begin to talk about the number of voters—millions of people, including seniors and people who can't even read. If it's not easy and convenient, it's just not going to happen to all of them. With the level of complexity that is involved in the voting process, it's no longer just about the basics. However, we now have to ensure data integrity, privacy of votes, and protection from all forms of cyber threats. Blockchain technology appears to be the next big thing—it's like putting votes in an unalterable and tamper-proof vault that cannot be changed. However, it's not a magic solution. You still need ways to know who is voting, how to identify fraud, and how to keep track of the whole system. Then there is quantum computing, which is coming soon and has the ability to break the encryption that we are currently using. Post-quantum cryptography exists, but at the moment, it is extremely expensive and hard to implement in the real world. Therefore, the plan is this: this project proposes a blockchain voting system that happens at polling stations, integrated with artificial intelligence and simulated post-quantum cryptography. It is meant to be local, so it hardly requires internet connectivity. By taking the tamper-proof element of blockchain technology and the intelligence and security of artificial intelligence that will be safe from quantum attacks in the future, this solution proposes a voting system that people can trust, one that is ready for academic research and, finally, safe use in the real world.

2. LITERATURE REVIEW

Overview

A lot of time has been spent trying to make electronic voting systems more secure, understandable, and speedy. "Old-school" methods, such as centralized databases or those pesky standalone voting machines, have been dissected for years. They're just too vulnerable to hacking, don't allow voters to verify their votes, and, honestly, they're not exactly confidence-builders. To address these issues, scientists applied cryptography, or digital signatures and secure hashing, to secure the votes. This means that one person in the know or one vulnerability can ruin it for the whole group. That's when blockchain came along. Now,

the concept of a decentralized voting system seems feasible. With the use of distributed ledgers, blockchain makes it difficult to hack and trace election data. Votes can't just magically disappear or change without leaving a trail, which is a great confidence-booster. However, the problem with blockchain is that it's not a magic solution either. It still has problems with large issues such as ensuring voters are who they claim to be, preventing people from being coerced or bribed, and detecting fraud as it occurs Fig (1). However, there is a new interest in artificial intelligence and machine learning. People are experimenting with these technologies to verify voter identities, detect unusual voting activity, and monitor the entire process Fig (2). These concepts are promising, but there is still a problem. AI and blockchain technology do not always play well together. Most of the current solutions have not quite figured out how to make these two technologies work well together.

Techniques Used in Existing Works

Most e-voting and blockchain-based voting systems rely very heavily on traditional cryptography and central verification to ensure that votes are secure. You can bet that you will see things such as traditional encryption, digital signatures, and hashing being used to secure votes and verify voters' identities. Of course, these are all fine against traditional cyber threats. However, research has shown that they are still vulnerable to things such as insiders manipulating election results, too much centralized power, and, more recently, the risk of quantum attacks. Additionally, many blockchain-based voting systems are very concerned with ensuring that votes cannot be altered later on, but then they forget about making it user-friendly and secure as people vote.

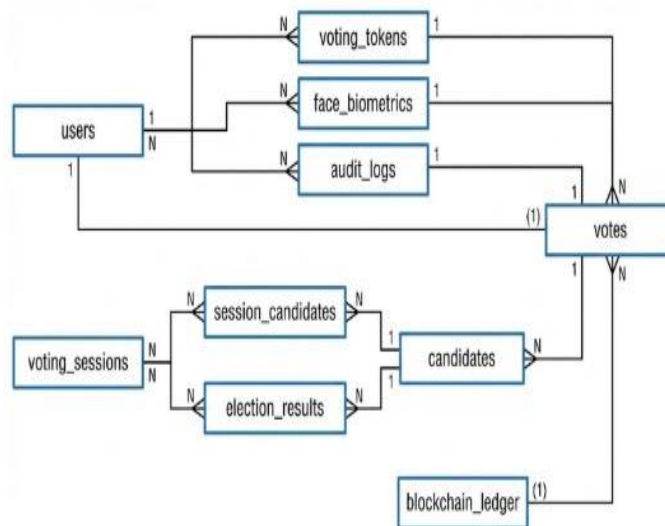


Fig (1)

Hybrid LLM and Model Handling Approaches

Hybrid security systems are very helpful in situations where you need something that is totally secure, like electronic voting, where security, privacy, and robustness are not just desirable but required. Here's how it's done: The system will perform its actual task, like voting, encrypting data, or keeping the blockchain, locally. That way, it won't have to depend on any external network, so even if the internet is down, the actual task will still be performed. However, when it comes to more complex tasks such as analysis and decision-making, the system can resort to the cloud or any other service, but only if it is

absolutely necessary. This kind of setup not only makes the system more robust, it also ensures that the system is cost-effective and that the sensitive information is where it should be: locked away. When it comes to voting systems, it is the local systems that do all the heavy lifting when it actually counts. The cloud only gets involved in system analysis, generating reports, or perhaps helping out with additional verification, but not the heavy lifting. This will also be the case with AI, where all the quick and easy verifications are done locally, but if there is a need for additional analysis, it calls on external sources.

Summary

Research People are becoming more and more interested in the use of blockchain technology and cryptography to enhance the security of electronic voting. However, most of what is available today does not really address the issues but rather is more of a smart eye on things as they go or keeping things secure as cryptography evolves. Of course, blockchain technology provides you with that immutable record, but many solutions have forgotten about smarter methods of verifying voters, detecting unusual activity, or automatically ensuring everything remains legit. That's what inspired us to develop our blockchain-based voting system. We introduced simulated post-quantum cryptography, AI-driven monitoring, and a single blockchain infrastructure—all in one—to develop something secure, transparent, and ready for whatever comes next.

3. PROBLEM DEFINITION AND RESEARCH OBJECTIVES

A. Problem Background:

Elections today are no longer just about electing leaders; they're also about trust. Citizens demand voting systems that are secure, transparent, and accessible to all. In India, conducting an election is a massive task. We are talking here about millions of voters from all over and from all walks of life. Of course, EVMs and VVPATs have certainly made the process faster compared to paper ballots, but serious concerns have not been alleviated. Questions about who is behind the system, how easily it can be audited, whether the technology will be able to withstand future attacks, and whether the common man trusts the system have not been answered. There's always a risk of cyber attacks, an insider attempting to hack the system, or even a future supercomputer that could break today's security. But there is a way forward. If we introduce new technology, such as blockchain, AI, and post-quantum cryptography, we can make it even more secure. And we can do this without making it more difficult for voters at the polling booth. The right technology not only secures the vote, but it helps people believe that the vote is real.

B. Challenges:

Let's face it—traditional voting methods have some serious issues. Most of them require a central hub, which essentially means that if something goes wrong there, the whole process can go south. This also gives people on the inside the opportunity to interfere with the voting process or even take control. In addition to that, traditional voting methods are not the best at detecting fraud as it is happening. They do not recognize unusual voting activity or alert someone to suspicious activity in real time, which means problems can fall through the cracks while the voting is taking place. And then there's this other pain point: cryptographic security. The encryption that we are using today may not be secure for a long time. This is because quantum computing is advancing rapidly, and the algorithms that we are using today may become obsolete. And then there are blockchain-based voting systems. Yes, they sound very promising,

but most of them require you to be online all the time. This is not very practical when it comes to secure polling stations, where you may have to work offline or have poor connectivity.

C. Research Objectives:

- To develop a private and blockchain-based voting system with the ability to securely and non-editably store votes.
- To incorporate artificial intelligence methods for voter verification, monitoring, and anomaly detection.
- To apply post-quantum cryptographic ideas via low-cost simulation using Python cryptographic libraries.

D. Scope and Significance:

Scope: The proposed system is more geared towards controlled environments of polling stations as opposed to internet voting. It is capable of simulating post-quantum cryptography, AI-based monitoring, and a private blockchain ledger, which makes it ideal for academic verification and pilot elections.

Importance: The system improves voter trust, transparency, future-proof security, and decreases the need for centralized monitoring. The system also exemplifies how innovative technologies can be integrated in a cost-effective and feasible way for next-generation electronic voting systems.

4. PROPOSED METHODOLOGY AND SYSTEM ARCHITECTURE

1) Input/Output Handler

The interface between the user and the system is provided by the input/output handler Fig (2). With its terminal-based interaction model, users can describe hardware in natural language and get Verilog code and diagnostic feedback.

- Uses common input mechanisms, such as Python or C++ input functions, to accept user input at runtime.
- The terminal shows the generated Verilog HDL code directly.
- Provides thorough error messages in the event of synthesis or simulation failures.

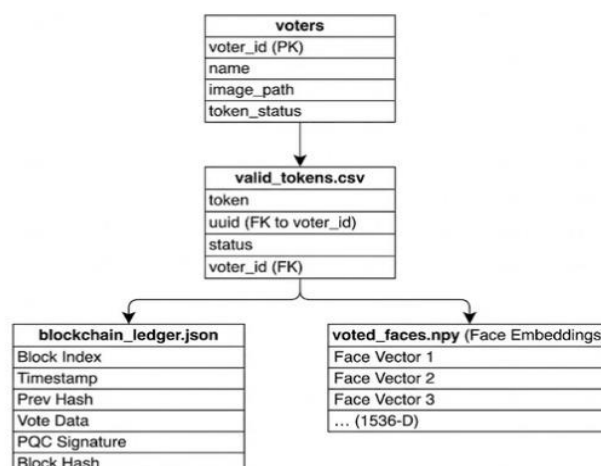


Fig (2)

2) Processing Module

- Uses NLP techniques to deconstruct natural language descriptions into structured parts.
- Recognizes hardware components like logic blocks, registers, inputs/outputs, modules, and signals.
- Transforms unstructured text into a prompt format that is standardized and compatible with LLM.

3) AI / Model Handling Module

- To ensure privacy, low latency, and offline operability, preliminary Verilog code drafts are generated using an offline LLM. Fig (3)
- For sophisticated error correction, optimization, and complex logic refinement, an online or hybrid LLM is used.
- Uses input from the synthesis and simulation phases to carry out iterative refinement.

4) Simulation Module

- Uses testbenches to carry out simulations.
- Identifies functional inconsistencies, timing infractions, and syntax errors.
- Facilitates sequential and combinational circuit verification.

5) Synthesis Module

- Generates gate-level netlists through syntax-checked synthesis.
- Recognizes warnings and synthesis errors.
- Optimizes performance metrics like logic depth, clock frequency, and resource usage. Fig (4)

6) Error-Correction Module

- Analyzes the errors reported by the synthesis and simulation modules.
- Points out the exact code segments that are causing errors.
- Supplies the LLMs with corrective instructions. The Verilog code is improved step by step until the errors are eliminated.

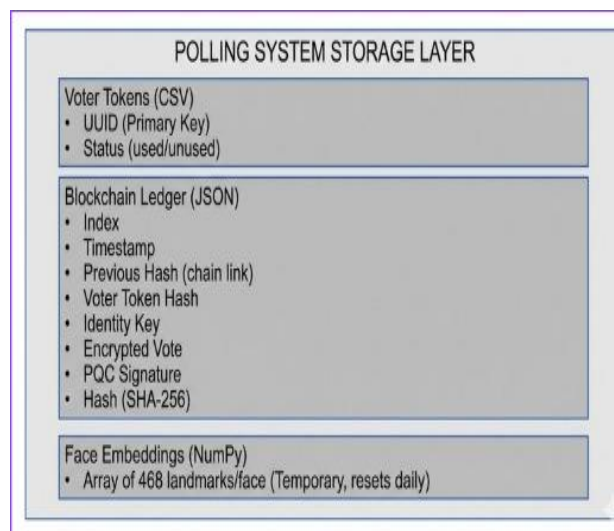
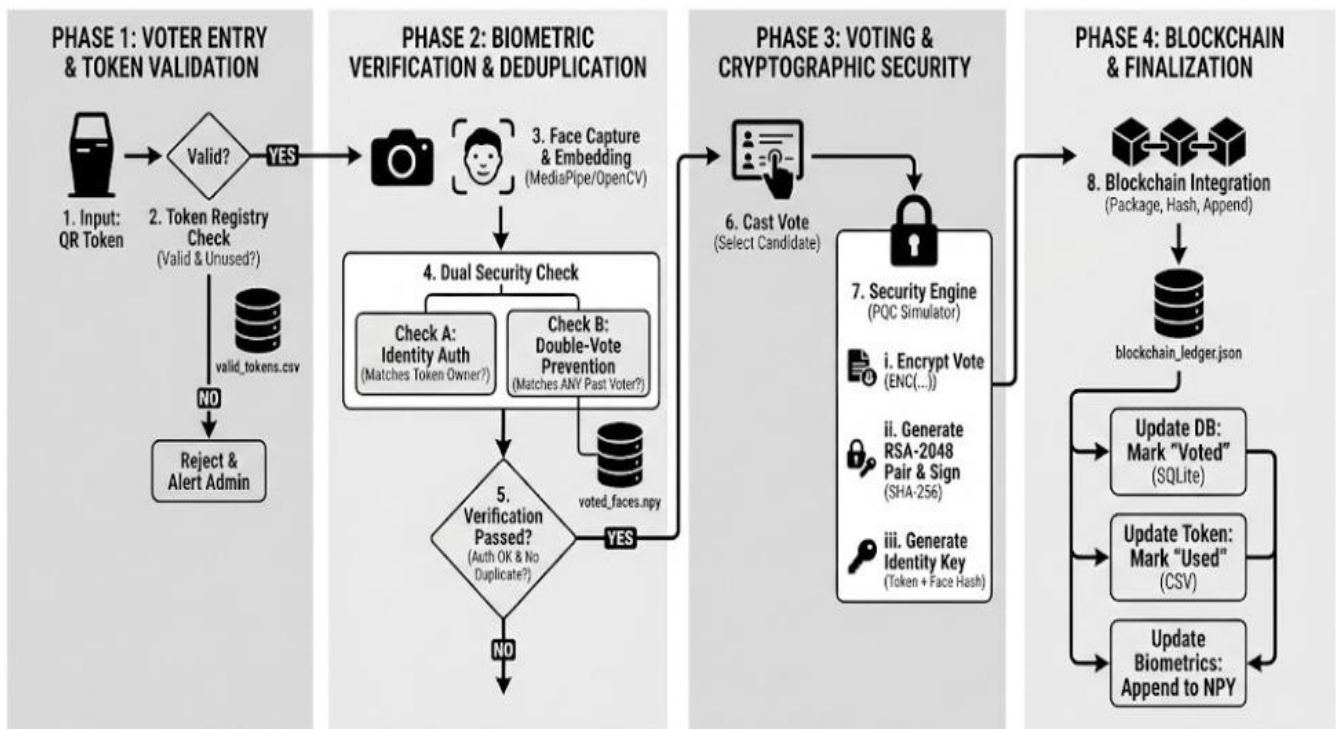


Fig (3)

Component	Technology / Library
Programming Language	Python 3.8+
Web Framework	Flask
Computer Vision Library	OpenCV
Face Recognition	MediaPipe
Cryptography Library	PyCryptodome
QR Code Generation	qrcode
Database	SQLite3 (built-in)

Fig (4)



5. RESULTS AND DISCUSSION

In the controlled testing environment, the proposed blockchain voting system was proven to be secure, transparent, and working for vote management. The process of vote transaction recording on the private Python blockchain was successful using the immutable hash verification technique, ensuring that the data is secure and tamper-proof. The simulated Post-Quantum Cryptography system was successful in creating secure digital signatures and encrypting vote information, hence being theoretically resistant to possible quantum attacks in the future. The votes were securely stored locally and synchronized with the blockchain using the offline-first architecture, hence proving its feasibility in polling stations where there is no constant internet connection. The blockchain voting system designed in this research was successful in implementing the real-time recording of votes and the display of results. As shown in the output interface, the live election results screen is able to dynamically display the distribution of votes among the candidates using a bar chart display. In the test environment, a total of 6 votes were placed, with Party A at the top,

followed by Party C and Party B Fig (5). The display of the results is easy to understand, ensuring that the results are transparent and clear to the election officials. The screen showing the blockchain ledger is capable of ensuring that the vote transactions are stored safely by verifying that the integrity of the data is maintained. Each vote is processed after token verification by the voter identification module, ensuring that only authorized individuals are able to cast their votes. The status indicator for the system, which shows “ONLINE,” ensures that the system is ready for use. The addition of Post-Quantum Cryptography to the system ensures that the conceptual security of the vote data stored in the system is maintained. The design of the dashboard is also improved, ensuring that the administrators are able to access the voting statistics and the ledger directly. The system is a perfect mix of transparency, security, and usability, ensuring the feasibility of the system in a controlled environment.

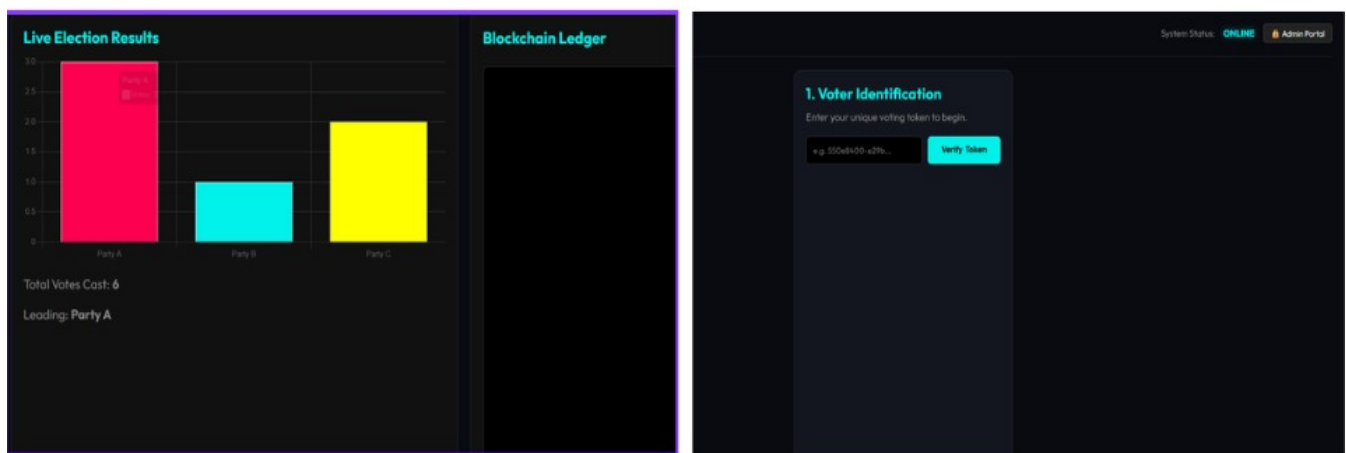


Fig (5)

6. ACKNOWLEDGEMENT

The authors would like to express their gratitude to **Dr. M Krishnamurthy, Head of Department, Department of AI & DS**, for her valuable guidance and supervision throughout the development of this project. The research was conducted as part of the **AD3811 Project Work (2025—2026)**, Department of Artificial Intelligence and Data Science, KCG College Of Technology, India.

REFERENCES

1. Pérez García, J. C., Benslimane, A., & Boutalbi, S. (2021). Blockchain-based system for e-voting using blind signature protocol. Laboratoire Informatique d'Avignon (LIA), Avignon University, Avignon, France.
2. Kamran, M., Nasir, M. H., Imran, M., & Yang, J.-S. (2021). Study on e-voting systems: A blockchain-based approach. Proceedings of the 2021 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia), 1–6. IEEE. DOI: 10.1109/ICCE-Asia53811.2021.9641914
3. Adiputra, C. K., Hjort, R., & Sato, H. (2020). A proposal of blockchain-based electronic voting system. Department of Electrical Engineering and Information Systems, The University of Tokyo, Tokyo, Japan.
4. Yang, Y., Guan, Z., Wan, Z., Weng, J., Pang, H. H., & Deng, R. H. (2021). PriScore: Blockchain-based self-tallying election system supporting score voting. IEEE Transactions on Information Forensics and Security, 16, 4705–4720. DOI: 10.1109/TIFS.2021.3108494

5. Venket, K., Ambica, A., & Freeda, A. R. (2024). Meta-Heuristics Algorithm for Computer Communications. In *Metaheuristic and Machine Learning Optimization Strategies for Complex Systems* (pp. 123-136). IGI Global.
6. Venket, K., Freeda, A. R., & Vijay, F. (2025). AI for Large-Scale Communication Networks. In *AI for Large Scale Communication Networks* (pp. 25-44). IGI Global.
7. Ashraf, N., Aftab, A., Qureshi, H. K., Kazim, M., et al. (2020, November). Machine learning with blockchain for secure e-voting system. In *Proceedings of the 2020 First International Conference on Smart Systems and Emerging Technologies (SMART-TECH)*. IEEE. DOI: 10.1109/SMART-TECH49988.2020.00050
8. Gao, S., Zheng, D., Guo, R., Jing, C., & Hu, C. (2019). An Anti-Quantum E-Voting Protocol in Blockchain With Audit Function. *IEEE Access*, 7, 115304–115316. DOI: 10.1109/ACCESS.2019.2935895
9. Poudel, A., Poudel, U., Aryal, D., Nepal, A., Pathak, P., & Subramaniaswamy, V. (2025, November). A quantum-secure and blockchain-integrated e-voting framework with identity validation. *ArXiv preprint arXiv:2511.16034*. DOI/Identifier: arXiv:2511.16034
10. Gajal, P., & Gautam, S. (2022). Blockchain-Based Voting System Using Quantum-Resistant Cryptography. In *Proceedings of the International Conference on Intelligent Systems and Smart Technologies* (pp. 211–219). IEEE.
11. Venkatraman, R., Kumar, S., & Iyer, P. (2022). Blockchain for Securing Electronic Voting Systems: A Survey. *Cluster Computing*, 25(4), 2789–2810. Springer.
12. Al-Mashaqbeh, I., Al-Hammouri, A., & Darwish, O. (2023). Blockchain-Based E-Voting Systems: A Technology Review. *Electronics*, 13(1), 17. MDPI.
13. Wang, J., Liu, Y., & Zhang, H. (2023). Efficient Lattice-Based Traceable Ring Signature Scheme for Secure Voting Systems. *Information Sciences*, 646, 119536. Elsevier.
14. Kaur, M., Singh, R., & Bansal, A. (2023). End-to-End Secure E-Voting Using Blockchain and Quantum Key Distribution. *Journal of Information Security and Applications*, 68, 103254. Elsevier.
15. Freeda, A. R., Ambica, A., & Venket, K. (2024). Hybrid Blockchain-Based Electronic Voting Machine Using Post-Quantum Cryptography. *Cryptography*, 2(4), 17. MDPI.
15. Ahmed, S., Rahman, M., & Hossain, M. (2024). Blockchain-Based E-Voting Mechanisms: A Survey and Comparative Analysis. *Digital Government: Research and Practice*, 4(4), 21. ACM.
16. Zhou, L., Chen, X., & Li, K. (2024). More Efficient Lattice-Based Electronic Voting from NTRU. *IEEE Access*, 12, 145233–145245. IEEE.
17. Banerjee, S., Das, A., & Mukherjee, D. (2024). Post-Quantum Blockchain Security: Survey and Research Directions. *Future Generation Computer Systems*, 151, 312–328. Elsevier.
18. Patel, R., Mehta, N., & Shah, V. (2024). Performance Evaluation of Post-Quantum Cryptography in Blockchain Networks. *Computer Communications*, 215, 124–136. Elsevier.
19. National Institute of Standards and Technology. (2023). Post-Quantum Cryptography Standardization: Digital Signature Schemes. NIST Technical Report, U.S. Department of Commerce.
20. Li, Y., Sun, Q., & Wang, T. (2025). Certificate-Less Linkable Ring Signature Schemes for Secure Blockchain Voting. *Computer Standards & Interfaces*, 89, 103782. Elsevier.
21. Rao, P., Srinivasan, K., & Iyer, R. (2025). PQC-VE: A Post-Quantum Framework for End-to-End Verifiable Electronic Voting. *TechRxiv Preprint*. IEEE.

22. Hassan, M., Al-Rashid, A., & Khan, F. (2025). AmarVote: A Web-Based ElectionGuard System with Post-Quantum Enhancements. In Proceedings of the ACM Conference on Secure and Trustworthy Systems (pp. 88–101). ACM.
23. Müller, T., Schneider, J., & Hofmann, M. (2026). Practical Post-Quantum Voting Protocols on Blockchain Architectures. IEEE Transactions on Dependable and Secure Computing, 23(1), 45–58. IEEE.