POWER MONITORING FOR OFFLINE BLOCKCHAIN VOTING: MQTT-DRIVEN REAL-TIME UPS MONITIORING AND LOCAL BACKUP

SUBMITTED BY:

UGBOR EBUBECHUKWU GABRIEL

211103090

SUBMITTED TO:

DEPARTMENT OF COMPUTER SCIENCE,

FACULTY OF COMPUTING,

NILE UNIVERSITY OF NIGERIA

IN PARTIAL FULFILMENT FOR THE AWARD OF BACHELOR OF COMPUTER SCIENCE (B.Sc.) DEGREE IN COMPUTER SCIENCE IN THE FACULTY OF COMPUTING

JANUARY 2025

MRS. AISHA LAWAL

ACKNOWLEDGMENT

I would like to express my deepest gratitude to the following individuals and organizations for their invaluable support and contributions to this project:

• **God**: For supporting me throughout my academic journey and allowing me to complete this work with sincerity and dedication.

• **My Supervisor**: Mrs. Aisha Lawal, for her guidance, expertise, and unwavering support throughout this journey.

• **My Teammate**: Amarachi Austin-okon, Hauwa Largema and Rahmat Jibril, for their collaboration, hard work and assistance towards the completion of the project.

• **My Family and Friends**: Nnenna, Kelechi, Amuche, Ginika and Chisom for their endless encouragement, understanding, and patience.

• **My Sponsors**: I thank my parents for their financial support, which made this project possible.

Their support has been instrumental in every step of this endeavor, and I am profoundly thankful for their presence in my life

DEDICATION

I dedicate this project to my lord and savior Jesus Christ, for guiding me throughout this journey and for letting me live in great health, focus, strength, knowledge, and determination to carry out this work. I also dedicate this work to my highly supportive family and friends, who stayed by me through the complete years of my degree.

ABSTRACT

This study investigates the design and implementation of an application layer for blockchain-based voting systems, specifically tailored to address infrastructural challenges in developing regions. The research identifies critical problems, including unreliable power supplies, limited internet connectivity, and poor user experience. To overcome these, the proposed system incorporates offline voting capabilities, robust synchronization mechanisms, and user-friendly interfaces. Employing a modular design, the application ensures scalability, security, and transparency, with advanced encryption and blockchain integration providing a tamper-proof audit trail. Simulated testing validates the system's resilience under adverse conditions, demonstrating its potential to enhance electoral integrity and foster voter confidence. This work serves as a blueprint for deploying reliable and scalable blockchain-based voting solutions in resource-constrained environments, bridging existing gaps in research and practice.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

The development of blockchain has brought absolutely new prospects to records management improvement concerning its transparency, safety, and credibility in general, including in the sphere of voting. Blockchain-based voting systems ensure record immutability, are fully decentralized, and feature increased security-a perfect solution to problems plaguing conventional voting mechanisms **[2]**. At the same time, the critical challenges these systems undergo include unsatisfactory infrastructure, particularly unsteady power supplies and poor internet connectivity, especially in developing regions.

In developing regions, such as Nigeria, these infrastructural gaps have always disrupted electoral processes, eroding confidence in the system and disenfranchising voters. The 2023 Nigerian elections were a reminder of these vulnerabilities, with numerous reports of technical failures arising from power outages and connectivity issues. The consequences of such disruptions are deep: delays in vote tallying, heightened risks of electoral fraud, and a general erosion of public confidence in democratic processes **[21][25]**.

This paper aims to address the challenges mentioned above within the application layer of blockchain-based voting systems. Utilizing robust software solutions, the work intends to ensure that it functions continuously even in adverse conditions, while maintaining data integrity and an ideal user experience **[9]**. Because most application layers face or interact directly with end-users, they include functions such as voter registration, ballot submission, vote encryption, and result verification **[18][22]**.

1.2 Motivation

Elections are the bedrock of democracy, and their integrity must be protected. The reason for this study lies in the imperative to protect democratic processes by overcoming infrastructural and systemic limitations. In the 2023 elections held in Nigeria, technological setbacks, such as unstable power supply and internet connectivity, revealed critical vulnerabilities in existing electronic voting systems **[16]**. These issues not only halted the voting process but also cast a shadow of doubt on the credibility and justice of the electoral system.

A well-designed application layer can then address these issues, including the support of features for offline voting capability, real-time synchronization with nodes in the blockchain, and simple interfaces for users and administrators alike. This study aims to contribute to the construction of a software solution that integrates all these points to ensure strong and reliable use of blockchain-based voting systems **[20]**.

1.3 Problem Statement

Elections are the bedrock of democracy, but in developing regions, infrastructural shortcomings and inefficient systems always seem to destroy their integrity. Frequent power outages and low internet connectivity in countries like Nigeria disrupt the processes of elections and cause delays, data loss, and a general loss of public confidence in the outcome of elections **[3][5]**. Matters are made worse by poorly designed interfaces: under resource-limited conditions, such an interface diminishes both voter accessibility and administrative efficiency **[19]**.

While these blockchains-based voting systems exist that foster security, transparency, and decentralization, they yet require stable infrastructures and have limited offline capabilities, hence not suitable for areas where the supplies of power and the internet are not reliable **[8]**

[15]. The scalability issues, high computational costs, and non-user-friendly interfaces of such systems prohibit their use in large-scale elections **[10][26]**. Despite advances in blockchain technology, critical gaps remain in ensuring seamless operation during outages and in integrating offline synchronization mechanisms to maintain data integrity **[12][28]**. In this respect, there is a great need to develop a blockchain-based voting system that could work in very adverse conditions since no robust, reliable, and accessible voting solution exists for developing regions. This project tries to respond to these challenges by embedding the capacity for offline voting, real-time synchronization, and user-friendly interfaces to advance electoral integrity and foster trust in democratic processes.

1.4 Aim and Objectives

- **Aim:** To design and implement an application layer for a blockchain-based voting system.
- **Objectives:**
    1. Design a secure voter interface for registration, ballot casting, and result viewing.
    2. Implement real-time communication protocols between the application layer and blockchain nodes to ensure data consistency.
    3. Implement offline voting capabilities with automated synchronization once connectivity is restored.
    4. Test the application under simulated adverse conditions to validate its resilience and performance.

1.5 Scope of the Study

The scope of this study is limited to the software aspect of a blockchain-based voting system, specifically focusing on the application layer.

1.6 Significance of the Study

The proposed application layer addresses critical issues in the deployment of blockchain-based voting systems in developing regions. By ensuring system reliability and data integrity, the solution fosters trust in the electoral process and enhances voter confidence **[10]**. The inclusion of offline capabilities and robust synchronization mechanisms ensures uninterrupted voting operations, even in adverse infrastructural conditions **[21]**.

Moreover, the system's modular design allows for scalability, making it adaptable to varying electoral requirements and infrastructural constraints. Advanced encryption techniques and blockchain integration provide a tamper-proof audit trail, enhancing the credibility and transparency of election outcomes. Lastly, this research serves as a blueprint for other regions facing similar challenges, paving the way for widespread adoption of secure and reliable electronic voting systems **[26]**.

1.7 Limitations of the Study

The study focuses on the application layer of blockchain-based voting systems and does not address hardware or infrastructural upgrades required for successful implementation. Challenges such as voter accessibility to devices, the cost of deploying blockchain technology, and potential resistance from stakeholders to adopt new systems are outside the direct scope of this research. Additionally, testing under real-world conditions is limited to simulations, which might not fully capture all environmental variables present in actual elections.

1.8 Definition of Terms

1. **Blockchain:** A decentralized, distributed ledger technology that records transactions securely and immutably. In this project, it ensures transparency and integrity in the voting process.
2. **Application Layer:** The user-facing component of a system that facilitates interaction with the underlying blockchain infrastructure for tasks such as voter registration and ballot submission.
3. **Offline Voting:** The capability to cast votes without an active internet connection, with data synchronized once connectivity is restored.
4. **MQTT (Message Queuing Telemetry Transport):** A lightweight messaging protocol designed for real-time data transfer in low-bandwidth environments, used for power monitoring in this system.
5. **Synchronization:** The process of aligning offline voting data with the blockchain network to ensure data integrity after connectivity is re-established.

CHAPTER TWO

LITERATURE REVIEW

This chapter reviews existing literature on blockchain-based voting systems, IoT-based power monitoring, and data synchronization methodologies. The goal is to identify gaps in current research and demonstrate how the proposed application layer addresses these challenges. By analyzing related works, this chapter provides a foundation for understanding the significance and innovation of the proposed solution.

2.1 Review on the Area of Project

The research work is built upon blockchain technology in order to increase the reliability and trustworthiness of electronic voting systems, mainly in developing democracies. It discusses the block creation mechanism, various sealing techniques, and the consortium blockchain maintained by election authorities in securing the voting process. SHA-256 for hashing and adaptable blockchain methods for improved scalability and trustworthiness are embedded into the framework. However, the existence of such limitations as result delay and lack of transparency in private blockchains is recognized and a customized "Proof of Completeness" algorithm is proposed to mitigate these shortcomings. **[2]**

This paper presents research findings on blockchain-based e-voting systems for their potentials to eliminate problems such as fraud, vote tampering, and absence of transparency in traditional voting. In this paper, a secure framework is proposed using smart contracts that automates the processes of voting for security. Usability aspects, however, remain challenging in blockchain systems for non-technical voters. **[4]**

This paper provides a structured review of some blockchain applications related to e-voting, mainly with respect to scalability and performance. It underlines several of the challenges confronted by blockchain-based voting, such as transaction speed, privacy, and cost, while discussing some already existing cryptographic solutions. The work outlines future lines of research to be pursued, optimization of consensus algorithms, and incorporating directed acyclic graphs, hence making it highly relevant for developing regions with sparse infrastructure. It emphasizes the use of scalable solutions to meet such an environment. **[7]**

This paper introduces a more advanced blockchain-based framework to augment evoting. The votes are safeguarded through cryptic keys and tamper-proof personal IDs in electronic voting. The voters will be given digital wallets, and every vote would be treated as a transaction, thereby ensuring an indelible audit trail. It would be flexible in that votes could be changed before any deadline. **[13]**

This paper emphasizes the fact that, through blockchain, electronic voting can be made safe, transparent, and decentralized, keeping the privacy of the voters via cryptographic techniques, including blind signatures and homomorphic encryption. The paper discusses various challenges regarding scalability, protection of voters' privacy, and transaction speed, while again emphasizing the potentials of blockchain for the replacement of centralized systems. However, gaps in frameworks for eligibility verification and real-world scalability remain critical areas for improvement. **[15]**

This survey assesses the feasibility of integrating blockchain into e-voting, addressing key challenges such as anonymity, secure identity management, and vote verifiability. While blockchain ensures integrity and decentralization, this article points out that it faces challenges like high deployment costs and vulnerability to cyberattacks. Case studies of global implementations, such as Estonia, showcase successes and gaps in current systems.

The study calls for further maturity of blockchain to ensure that e-voting systems are reliable and scalable. **[23]**

This paper will address the issue of using blockchain for the enhancement of trust and reliability in electronic voting systems, particularly in developing democracies. It describes block creation, sealing techniques, and using consortium blockchain, managed by the election authorities, to secure the voting process. The framework integrates SHA-256 for hashing and adjustable blockchain methods for better scalability and trustworthiness. However, result delays and a lack of transparency in private blockchains are identified issues, which a specifically designed "Proof of Completeness" algorithm is suggested to overcome. **[29]**

2.2 Review on Technologies

This study develops a blockchain-based solution for file synchronization, thereby strengthening data integrity and operation resilience. Integration of blockchain characteristics, such as immutability, distributed architecture, and user authentication, is incorporated into it for efficient version control and data synchronization even with decentralized networks. This solution does not rely on centralized servers to make it resistant to failures. Proof-of-work mechanisms secure data, making key benefits include more fault tolerance and a lower reliance on external operations. **[1]**

It designs a blockchain-based framework with face verification and implements smart contracts for secured transparent voting. It improves the trust in the current system by ensuring that the data is tamper-proof and verifiable, reducing the possibility of fraud. Challenges include the high computational requirements of blockchain technology and accessibility for large-scale populations. **[5]**

This paper proposed a blockchain-based e-voting protocol ensuring transparency and privacy in the voting process. Main features contributed here are a possibility of changing one's vote during the election period, a transparent digital ballot box, and individual verifiability. Though this represents a practical challenge to implement due to computational limitations in blockchain, the potential for improved voter trust in the process and system reliability are proposed as proof of the protocol. This will directly contribute to the project's objectives of securing and ensuring reliable systems in resource-constrained settings. **[8]**

This review highlights some gaps in the e-voting systems and assesses blockchain for its potential to fill those gaps. It identifies challenges such as transaction speed, privacy, scalability, and the need for robust consensus models. While blockchain indeed offers immutability, decentralized ledgers, and enhanced data integrity, challenges persist, such as 51% attacks, transaction speed, and privacy concerns. The study therefore calls for the enhancement of frameworks for secure and scalable e-voting. **[10]**

This research presents the blockchain-based voting system for use on the internet on the Ethereum base with smart contract. It refers to the impermeability of blockchains and therefore the security involved in cryptographic operations. The proposed solution ensures anonymity; however, all voters can only be verified on the basis of biometric credentials. Scalability and high costs related to transaction validation "gas" charged by Ethereum prevent the system. **[12]**

It suggests an e-voting system based on Hyperledger Fabric, with efficiency, security, and scalability ensured through permissioned blockchains. The efficiency of such a system is enhanced by elimination of the traditional consensus mechanism, access control, and hence, secure vote management through smart contracts. Despite practicality, the challenges related to voter accessibility and large-scale election scalability are now evident in the study. **[16]**

The research proposes a decentralized voting platform based on the Ethereum blockchain using MetaMask for voter registration and voting. Voting tokens are given to the registered users, which are utilized in casting votes on the blockchain, ensuring transparency and immutability. The automation of vote tallying makes the election process much easier, avoiding the manual counting of votes. Though the framework is innovative, it still remains theoretical and has not been deployed at large. The challenges include user accessibility and usability by non-technical participants. **[19]**

It makes emphasis on using private blockchain in electronic voting as secure and dependable. This method integrates cryptographic algorithms and private blockchain to overcome challenges such as tampering with data, double voting, and lack of trust in centralised systems. A system with properties such as privacy for the voter, eligibility checking, and encrypting the transfer of data is put forward. This system utilizes Practical Byzantine Fault Tolerance in order to create a consensus and hinder malicious actions. The study highlights significant improvements in data integrity and scalability compared to traditional methods. **[21]**

This research proposes a permissioned blockchain-based e-voting system for resolving challenges inherent in traditional electoral processes that include vote tampering and lack of transparency. It incorporates distributed ledger technology, end-to-end verifiability, and cryptographic techniques such as SHA-256 for data integrity. It tries to outline the potential role of blockchains regarding tamper-proof, transparent elections. Limitations are the high initial setup cost, infrastructure requirements, and unresolved issues on accessibility for rural populations. **[25]**

This paper focuses on the use of blockchain to address issues of transparency and auditability in voting. Here, the study introduces the ABVS, using intelligent agents that enhance security and efficiency. Emphasis is on the role played by multi-agent systems in validation of data reliability and process integrity. The proposed model of the ABVS contains super-nodes and trusted nodes, which resonate with the vision of reliability even during outages. **[32]**

The paper describes how blockchain can overcome some of the security and transparency problems of elections. It proposes a decentralized system whereby voters' identities will remain secret and the voting is cast safely by a smart-card and one-time password mechanism. Providing voter authentication, data confidentiality, and real-time results through the use of the ElGamal cryptosystem for encryption and SHA-256 for hashing, this system does have many merits. The challenges it faces include requirements of accessible technology and public adoption in developing regions. [ ]

2.3 Existing Projects

The current work investigates protocols for achieving full voter privacy without recourse to trusted third parties. It looks into the distributed algorithms ensuring the security of election outcomes while keeping anonymity and avoiding vote manipulation. It takes note of some impossibility results regarding unconditional privacy in specific schemes and proposes ways to achieve strong privacy guarantees under realistic assumptions. These might provide inspiration for mechanisms of offline synchronization for the project, helping to handle concerns about voter security in constrained environments. **[9]**

The authors propose a blockchain-based score voting system that ensures the privacy of the voters through zero-knowledge proof and encrypted transactions. It tries to mitigate challenges such as score manipulation and data integrity issues by validating the score range beforehand. Performance evaluations show scalability up to 10,000 participants, but computational and communication overheads have been pointed out as limitations. **[11]**

This paper proposes a decentralized, smart contract-based e-voting system on the Ethereum platform that ensures privacy, integrity, and anonymity for voters. This system makes use of blockchain to develop a transparent ledger in which all votes are recorded, hence ensuring the integrity of the voting process. It uses RSA encryption and Merkle trees for secure data storage. Moreover, voters can verify their votes using transaction IDs. **[14]**

It introduces an e-voting system based on the sidechain which guarantees privacy, transparency, and verifiability using zero-knowledge proofs and Shamir's Secret Sharing. This system splits the voter registration and vote counting on linked blockchains, thus facilitating secure remote voting and traditional e-voting settings. Though innovative, it has shown some issues regarding scalability and practicability. **[17]**

This article proposes a blockchain-based system for e-voting on the Ethereum blockchain, through which smart contracts allow for secure and transparent elections by ensuring immutability. Through this system, voters can now vote using both Ethereum wallets or Android devices, and it validates each transaction in the blockchain network. The above approach ensures transparency and integrity because votes are immutable on the blockchain. However, the study has limitations in scalability for large-scale elections and challenges in maintaining voter anonymity. Moreover, voters require Ethereum wallets and small amounts of ether to participate. **[18]**

A model was designed for this research using the Ethereum blockchain along with the implementation language, Solidity. This model assures data integrity and transparency by securing election results in this blockchain. An interface has also been proposed here through a web-based environment in order to support voter authentication along with their vote submissions independently without depending on a centralized database. This mechanism has some bottlenecks concerning Internet requirements, Ethereum wallet availability, and ethers required as gas charges in Ethereum-based electronic ballot elections. **[20]**

This paper proposes an e-voting system empowered by blockchain that enhances the system's transparency, security, and scalability. The system relies on Ethereum-based smart contracts to manage registration, vote casting, counting, and donation processes. Major issues such as vote tampering, fraudulent voter detection, and cyberattacks will be tackled with this system. It offers users user-friendly GUIs and cryptocurrency wallets that increase accessibility and ease-of-use for users. The proposed architecture is highly adaptable and robust in conducting secure online elections. **[22]**

This paper researches the application of Ethereum-based blockchain technology for e-voting systems on secure, transparent, and decentralized mechanisms. The system uses smart contracts for managing the procedures of voting, maintaining the privacy of the vote, its immutability, and transparency. A prototype web application is provided, implementing the same in real life by enabling voter registration and verification of votes via OTP authentication. Limitations are pointed out regarding scalability to large-scale elections, as well as completely anonymizing voters with blockchain. **[24]**

The paper suggests an e-voting solution with the integration of Ethereum-based smart contracts for higher security and cost efficiency. This ensures voter privacy and transparency and addresses the issue of integrity within the process of voting. Biometric validation within a decentralized app will ensure that it is pretty robust with unique hash addresses for the voters. However, the study again points out scalability issues and the possible need for further adaptations to be efficient in large-scale elections. **[26]**

It describes a two-layer, decentralized architecture for voting and identification using blockchain for transparency with the anonymity of voters. This protocol describes steps involved right from the registration of voters to counting the results by ensuring fault tolerance, scalability, and secure authentication of voters. The identity and voting layer using permissioned blockchains forms a very relevant precedent on the reliability of the project in terms of its offline synchronization mechanisms. **[28]**

2.4 Existing Literature

This research investigates the integration of IoT devices in offline blockchain scenarios using the IOTA framework. It examines challenges in transaction synchronization and finality in partially synchronous networks. The IOTA-based solution will be used by applying the structure of DAG for offline operations and periodic data merging, which will meet scalability and low-cost transaction needs. Limitations: The system requires very precise time synchronization to avoid the problem of stale data. IoT nodes have limited resources. **[3]**

This survey conducts the evaluation of several blockchain-enabled e-voting systems on the level of scalability, security, and transparency improvements over traditional systems. It pinpoints usability and system adaptability gaps for large-scale elections and stresses blockchain's decentralized and immutable features as novel solutions towards currently created issues. **[6]**

The paper reviews the evolution of blockchain's application in voting, pointing out its decentralized, transparent, and secure attributes. Challenges such as computational overhead are pointed out, while blockchain maintains voter anonymity and integrity. Such insights guide addressing challenges of offline voting and synchronization issues. **[27]**

A blockchain-based e-voting system, using private Ethereum networks is proposed in this paper. This work focuses on voter registration, OTP authentication, and blockchain with MongoDB-based secure voting. It ensures eligibility for voters using smart contracts to avoid multiple votes. It might be efficient for smaller applications, but it lacks efficiency in consumption of resources and scalability in larger applications. **[31]**

2.5 Summary of Recent Works

Title	**Author and Year**	**Summary**	**Limitation**
Using Blockchain Technology for File Synchronization	Khan et al., 2019	Proposes a blockchain-based system for file synchronization, emphasizing immutability, distributed architecture, and version control.	Computational overhead due to proof-of-work and potential complexity in deployment.
Offline Scaling of IoT Devices in IOTA Blockchain	Rawat et al., 2022	Explores IOTA-based DAG ledger for offline IoT scalability, ensuring low-cost transactions and	Time synchronization challenges and risk of transaction staleness in partially connected IoT networks.

		support for partial synchronization.	
Electronic Voting System Powered by Blockchain Technology	Milan Ray et al., 2023	Discusses blockchain's role in combating fraud and ensuring transparency in e-voting via decentralized systems.	Complexity of use for non-technical voters and security challenges in certain system designs.
A Framework to Make Voting System Transparent Using Blockchain Technology	CH. Sunandini et al., 2020	Proposes a blockchain-based voting system with face verification and immutable smart contract functionalities.	High computational resource requirements and limited testing on large-scale populations.
Survey on Online E-voting System Using Blockchain Technology	Sangeeta Alagi et al., 2023	Reviews blockchain-based voting systems, highlighting security, scalability,	Limited research on usability and implementation challenges for large-scale voting.

		and transparency benefits.	
A Systematic Literature Review and Meta-Analysis on Scalable Blockchain-Based Electronic Voting Systems	Jafar, U., et al., 2022	This article reviews scalable blockchain-based voting systems, addressing issues such as authentication, privacy, integrity, and scalability. It identifies research directions like enhancing consensus algorithms for scalability.	Scalability remains an unsolved challenge, with limitations in transaction speed and consensus mechanisms
E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy	Hardwick, F. S., et al., 2016	Proposes a decentralized e-voting protocol using blockchain for transparency and privacy. Voters	Challenges include the need for a centralized authority for voter eligibility verification and

		can alter votes during elections, leveraging smart contracts for ballot storage while ensuring transparency and individual verifiability.	blockchain scalability issues.
Decentralized Voting with Unconditional Privacy	Brandt, F., and Sandholm, T., 2005	Explores protocols for achieving unconditional voter privacy without trusted third parties. Introduces distributed algorithms to maintain election outcome privacy while minimizing information leakage.	Impossibility results show unconditional full privacy cannot be achieved for many voting schemes; relies on specific assumptions.

A Systematic Review of Challenges and Opportunities of Blockchain for E-Voting	Ruhi Taş and Ömer Özgür Tanrıöver, 2020	This systematic review highlights blockchain's potential in addressing gaps in e-voting systems, focusing on immutability, decentralized ledgers, and data integrity. It emphasizes issues with privacy, transaction speed, and scalability, advocating for improved consensus mechanisms and frameworks.	Privacy concerns, scalability limitations, and vulnerabilities like 51% attacks remain unresolved.
Privacy-Preserving E-Voting System Supporting Score	Ali Alshehri et al., 2023	The paper introduces a blockchain-based	Computational and communication overheads pose

Voting Using Blockchain		e-voting system supporting score voting, ensuring privacy with zero-knowledge proofs. It validates score ranges to prevent manipulation and scales to 10,000 participants, demonstrating its efficiency for mid-sized elections.	challenges for larger-scale implementations.
Blockchain-Based Voting System with Ethereum Blockchain	Jinjie Chai, 2020	Proposes a blockchain-based voting system using Ethereum, ensuring transparency, anonymity, and verifiability with smart contracts.	High costs due to Ethereum's gas fees and potential vulnerabilities in smart contracts.
Trustworthy Electronic Voting	Elba Rajathi et al., 2023	Highlights an e-voting system using	Scalability challenges and

Using Adjusted Blockchain		an adjusted blockchain with secure cryptographic keys, allowing voters to change votes before a deadline.	vulnerability to real-time attacks like DDoS.
Decentralized E-Voting System Using Blockchain	Prajwal Shiwal et al., 2023	Discusses a decentralized e-voting system built on Ethereum with transparency, voter privacy, and integrity ensured by smart contracts and cryptographic methods.	Computational overhead limits large-scale adoption.
Blockchain for Electronic Voting System—Review and Open Research Challenges	Uzma Jafar, Mohd Juzaiddin Ab Aziz, Zarina Shukur, 2021	Explores blockchain's potential for secure, transparent, and decentralized	Limited scalability and transaction speed, and incomplete frameworks for eligibility

		voting systems, highlighting its cryptographic techniques (e.g., blind signatures, homomorphic encryption) to ensure voter privacy. Identifies its transformative role but notes gaps in scalability and privacy.	verification in large-scale implementations.
Electronic Voting System Using an Enterprise Blockchain	Camilo Denis González, Daniel Frias Mena, Alexi Massó Muñoz, Omar Rojas, Guillermo Sosa-Gómez, 2022	Proposes an e-voting system using Hyperledger Fabric to enhance efficiency and security through permissioned blockchains. Implements access control, smart	Scalability challenges in handling large-scale elections and issues related to voter accessibility, particularly in regions with limited digital literacy or resources.

		contracts, and modular architectures to balance decentralization and performance, demonstrating practical use in controlled environments.	
Crypto-voting: A Blockchain-Based E-Voting System	Francesco Fusco, Maria Ilaria Lunesu, Filippo Eros Pani, Andrea Pinna, 2018	Describes a two-sidechain e-voting system combining blockchain with Shamir's Secret Sharing for enhanced privacy and transparency. Separates registration and vote counting processes while enabling secure	Implementation remains at a prototype stage, with unresolved challenges in scalability, synchronization, and broader adoption in large and diverse electoral scenarios.

		remote and traditional e-voting setups.	
Towards Secure E-Voting Using Ethereum Blockchain	Ali Kaan Koç, Emre Yavuz, Umut Can Çabuk, Gökhan Dalkılıç, 2018	Proposes an e-voting system using Ethereum blockchain and smart contracts for secure, transparent, and immutable elections. Allows voting through Ethereum wallets or Android devices, ensuring vote integrity with blockchain consensus mechanisms.	Limited scalability for national-level elections and challenges in voter anonymity. Requires users to have Ethereum wallets and small amounts of ether.
Decentralized Voting: Ethereum-	Luke Reddick, 2018	Proposes a decentralized voting application	Implementation remains a theoretical

Based Voting Platform		using Ethereum blockchain and MetaMask for registration and voting. The system uses tokens to represent votes, leveraging blockchain immutability and transparency for secure voting and automated vote tallying.	framework with no full-scale deployment. Challenges include limited usability for non-technical voters.
Electronic Voting Using Decentralized System Based on Ethereum Blockchain	Missa Lamsani, Singgih Jatmiko, Fajri Fadli, 2020	Develops a decentralized e-voting system using Solidity and Ethereum blockchain to ensure data integrity and transparency. The	Requires an internet connection, Ethereum wallet setup, and ether for gas fees. Scalability and accessibility for large-scale

		system includes a web interface for voter authentication and secure vote storage on the blockchain.	elections remain concerns.
A Study on Electronic Voting System Using Private Blockchain	Chang-Hyun Roh C Im-Yeong Lee, 2020	This article explores the use of private blockchain for secure electronic voting. It incorporates cryptographic algorithms and PBFT consensus to address trust and data tampering. Ensures privacy, fairness, and data integrity with encryption mechanisms.	Limited scalability and challenges in extending processing speed for large-scale applications.

BCT-Voting: A Blockchain Technology-Based Voting System	Deepali Raikar C Avimanyou Vatsa, 2021	Proposes a blockchain-based e-voting system with Ethereum smart contracts. It includes modules for registration, vote casting, counting, and donation. The system aims to improve transparency, security, and user experience while addressing fraud detection.	Dependence on Ethereum increases transaction costs; the system's adaptability in low-connectivity regions is not addressed.
A Survey on Feasibility and Suitability of Blockchain Techniques for E-Voting Systems	Umut Can Çabuk et al., 2018	Surveys blockchain-based e-voting systems, highlighting their potential in ensuring	Limited practical implementation details and insufficient focus on offline or hybrid

		anonymity, integrity, and decentralization. It also discusses challenges like deployment costs, trust, and cyberattacks with case studies from different countries.	connectivity solutions.
E-Voting Using Blockchain Technology	Yadav et al., 2020	Proposes Ethereum-based e-voting with smart contracts for security and transparency. Demonstrates a prototype with OTP verification for voter authentication.	Scalability and voter anonymity remain challenges.

Blockchain Technology-Based E-Voting System	Lahane et al., 2020	Describes a permissioned blockchain framework for tamper-proof elections, using SHA-256 and distributed ledgers for end-to-end verifiability.	High initial costs and rural accessibility are concerns.
Blockchain-Based E-Voting System	Benny et al., 2020	Implements Ethereum-based voting with smart contracts, providing privacy and transparency. Utilizes biometric verification and unique hash addresses for authentication.	Scalability for nationwide elections is limited; further measures needed for high transaction throughput.
Towards the Intelligent Agents	Michał Pawlak et al., 2018	Introduces the Auditable	Limited exploration of scalability and

for Blockchain E-Voting System		Blockchain Voting System (ABVS) leveraging intelligent agents and multi-agent systems for secure and auditable e-voting.	handling intermittent connectivity in developing regions.
DemocracyGuard: Blockchain-Based Secure Voting Framework	Mritunjay S. Peelam et al., 2024	Proposes a blockchain-based secure voting system integrating Ethereum smart contracts and facial recognition for voter authentication.	Does not address offline voting scenarios and real-time synchronization during connectivity loss.
Decentralized Electronic Voting System Based on Blockchain	Kateryna Isirova et al., 2020	Proposes a two-level decentralized architecture using blockchain for voter identification and result counting	Relies heavily on pre-established internet connectivity and does not integrate

		with a six-step secure protocol.	UPS or power resilience.
Trustworthy Electronic Voting Using Adjusted Blockchain Technology	Basit Shahzad C Jon Crowcroft, 2019	Proposes an adjustable blockchain framework for e-voting, focusing on block creation, sealing, and consortium blockchain to enhance security, scalability, and voter trust.	Limited transparency in private blockchain and challenges in ensuring fairness for all stakeholders.
Blockchain-Based Secured E-Voting System	Md. Shahriare Arnob et al, 2020	Introduces a decentralized blockchain-based e-voting system using smart cards, OTP, and SHA-256 for secure voting and real-time result publishing to	Challenges in accessibility and adoption in resource-constrained regions.

		enhance transparency in elections.	
Blockchain-Based E-Voting Using Private Ethereum	Mrunal Pathak et al., 2021	Describes a private Ethereum-based e-voting solution with features like OTP-based authentication, smart contracts, and vote validation to address common e-voting issues.	Primarily suitable for small-scale elections; less effective for national elections.

Table 2.1 – Table Showing Summary of Recent Works

CHAPTER THREE

METHODOLOGY

This chapter outlines the system analysis and design methodology for the application layer of the blockchain-based voting system. It includes a detailed description of system requirements, design principles, architectural considerations, feasibility analysis, and implementation strategies. The application layer serves as the critical interface between end-users and the underlying blockchain infrastructure, ensuring seamless operation, data integrity, and security.

3.1 Description of the System

This project proposes the design and implementation of a blockchain-based voting system tailored to the challenges of developing regions. The system integrates offline voting capabilities, real-time power monitoring using MQTT, and a user-friendly interface. It is designed to operate seamlessly under adverse conditions, ensuring secure data synchronization and transparent election processes. Key components include the application layer for voter interaction, a blockchain layer for secure data recording, and a synchronization module for offline functionality.

System Requirements

The system requirements for the proposed application layer are categorized into functional, non-functional, hardware, and software requirements.

Hardware Requirements

1. **Client Devices:** Smartphones, tablets, or computers with internet access.
2. **Server Infrastructure:** High-performance servers with redundancy for handling requests and storing data.
3. **Backup Systems:** External SSD/HDD storage for local backups during outages.

Software Requirements

1. **Programming Languages:** Node.js (backend), React.js (frontend).
2. **Frameworks:** Express.js API development.
3. **Blockchain Platform:** Ethereum for permissionless blockchain operations.
4. **Database Management:** MongoDB for voter and election data storage.
5. **Communication Protocols:** MQTT for real-time messaging and synchronization.

3.2 SDLC (Software Development Life Cycle)

3.2.1 Possible/Candidate Methods

Several SDLC methodologies were considered for this project:

1. **Waterfall Model:** A linear, sequential approach suitable for well-defined projects but less adaptable to changes during development.
2. **Agile Methodology:** An iterative model emphasizing flexibility, continuous stakeholder involvement, and incremental delivery.

3. **Incremental Model:** A phased approach that delivers functional components in increments, enabling early testing and validation.

3.2.2 Adopted Methodology

The Waterfall methodology was chosen for this project due to its structured and sequential nature. It ensures that each phase—from requirement gathering to system deployment—is completed thoroughly before moving on to the next. This approach provides:

1. Clear documentation of requirements and design.
2. A well-defined timeline for project milestones.
3. Simplified tracking of progress, making it suitable for projects with clearly defined goals and deliverables.

3.3 Requirements Engineering

3.3.1 Requirement Gathering

The following methods were employed to gather system requirements:

1. **Stakeholder Interviews:** Engaged with potential users, including voters and administrators, to identify key functionalities and challenges.
2. **Surveys:** Conducted surveys to understand user expectations and infrastructural limitations.
3. **Literature Review:** Analyzed existing studies to identify gaps in current blockchain-based voting systems.

3.3.2 Functional and Non-functional Requirements

Functional Requirements

1. **User Authentication:** Secure login for voters and administrators using multi-factor authentication.
2. **Voter Registration:** A module for securely capturing and storing voter details.
3. **Ballot Casting:** A feature for voters to submit their votes through an intuitive interface.
4. **Offline Voting:** Support for offline voting with automated data synchronization upon connectivity restoration.
5. **Result Verification:** Real-time display of voting results with blockchain verification.
6. **Administrative Tools:** Dashboards for managing elections, monitoring voting activities, and resolving disputes.

Non-Functional Requirements

1. **Scalability:** Support for thousands of concurrent users without performance degradation.
2. **Usability:** A user-friendly interface designed for diverse literacy levels.
3. **Security:** Implementation of end-to-end encryption and blockchain-based data integrity checks.
4. **Reliability:** System resilience to power outages and network disruptions.
5. **Performance:** Real-time data processing with minimal latency.

3.3.3 Requirement Elicitation

Refinement of requirements was achieved through:

1. **Prototyping:** Developed low-fidelity prototypes to gather feedback.
2. **Focus Groups:** Organized sessions with stakeholders to validate features and workflows.
3. **Scenario Analysis:** Simulated adverse conditions to identify potential gaps and improve system design.

3.4 System Analysis

3.4.1 System Architecture

The proposed architecture integrates the following components:

1. **Frontend Layer:** Provides an intuitive user interface for voters and administrators.
2. **Backend Layer:** Manages application logic, API endpoints, and blockchain communication.
3. **Blockchain Layer:** Ensures secure and immutable recording of votes.
4. **Synchronization Layer:** Handles data synchronization between offline and online modes.

Deployment Diagram

The deployment diagram (Figure 3.3) represents the physical architecture of the system, showing how hardware and software components are connected in the operational environment. The key components include:

1. **Voter Device**:
    - Devices such as smartphones, tablets, or laptops used by voters to interact with the voting system.
    - Runs the frontend application and communicates with the backend server.
2. **Administrator Console**:
    - Devices used by administrators for monitoring, system management, and troubleshooting.
3. **Raspberry Pi**:
    - Acts as the edge device for power monitoring and communication with sensors.
    - Responsible for triggering backups during power disruptions.
4. **Sensors (PZEM-004T and ZMPT101B)**:
    - Monitor real-time power conditions and report data to the Raspberry Pi.
5. **Server Infrastructure**:
    - High-performance servers for backend processing, blockchain operations, and database management.
    - Includes redundancy mechanisms to handle system load and ensure reliability.
6. **External Backup Storage**:
    - SSDs or HDDs connected to the Raspberry Pi for storing backups during outages.
7. **Blockchain Network**:

    - Implements secure and immutable storage for voting records and power events.

Communication Flow:

- Voter devices communicate with the backend server via RESTful APIs.
- Raspberry Pi collects power data from sensors and sends updates to the server.
- Backup storage devices interact with the Raspberry Pi for real-time data preservation.
- The blockchain network records votes and power events for auditing and verification.

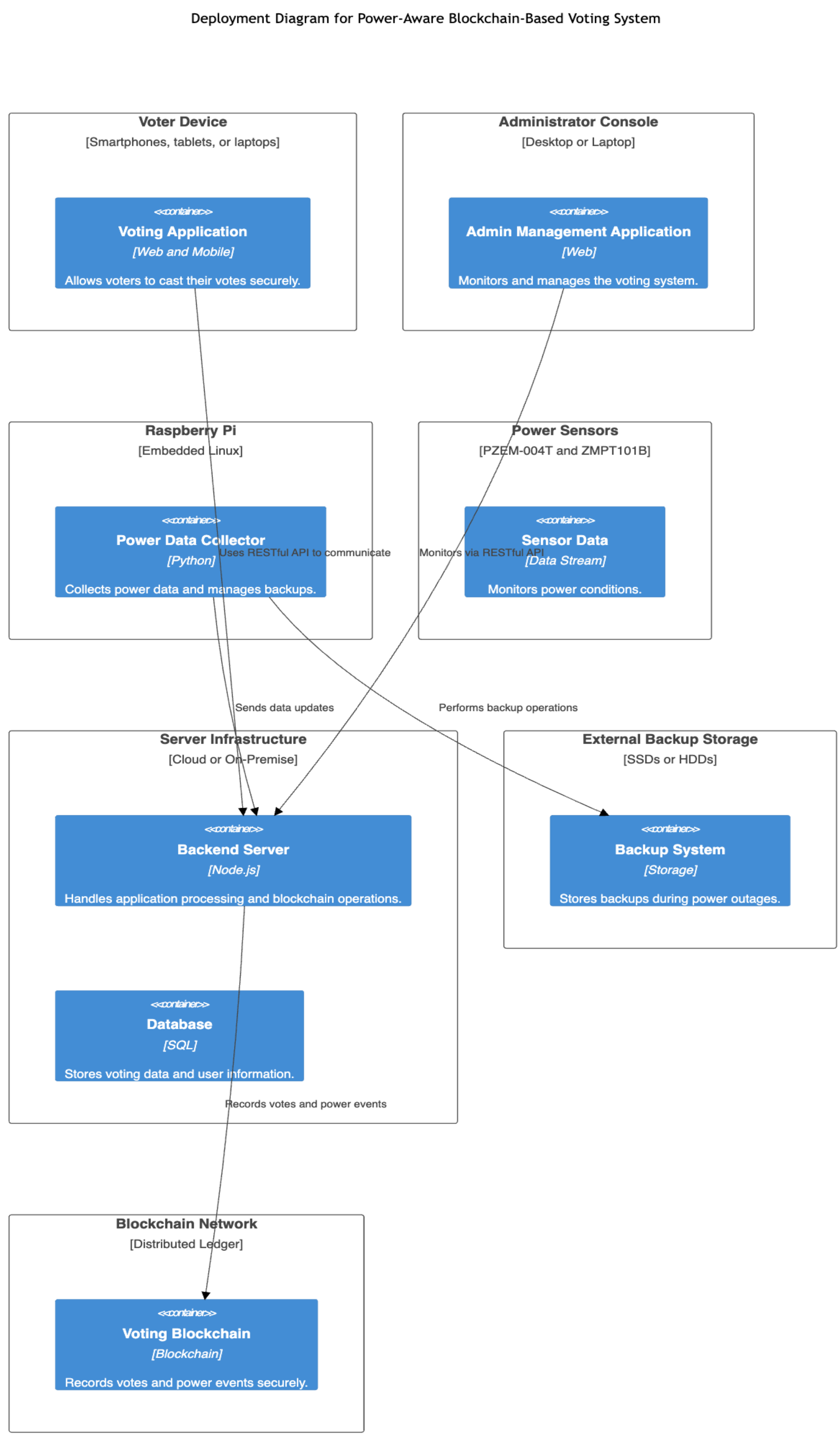

Figure 3.1 – Deployment Diagram of the Proposed System

The deployment diagram (Figure 3.1) provides an overview of the system's deployment architecture, detailing how hardware components (e.g., Raspberry Pi, UPS) and software modules are interconnected.

3.4.2 Use Case Diagram

The use case diagram visually represents the relationships between actors and the system's core functionalities. It ensures that all user interactions and responsibilities are clearly outlined and mapped to the appropriate system components.

Actors:

1. **Voter**:
   - Interacts with the system to register, log in, and cast votes.
2. **Administrator**:
   - Monitors the system, reviews logs, and ensures operational continuity.

Use Cases:

- **Register as Voter**: The Voter provides personal details to create an account.
- **Log in to System**: Both Voter and Administrator authenticate themselves.
- **Cast a Vote**: The Voter selects a candidate and submits the vote.
- **Monitor System**: The Administrator reviews system performance and logs.
- **Handle Power Events**: The system detects power disruptions and initiates backups, with the Administrator overseeing the process.
- **Verify Votes**: The Administrator reviews voting data for integrity.

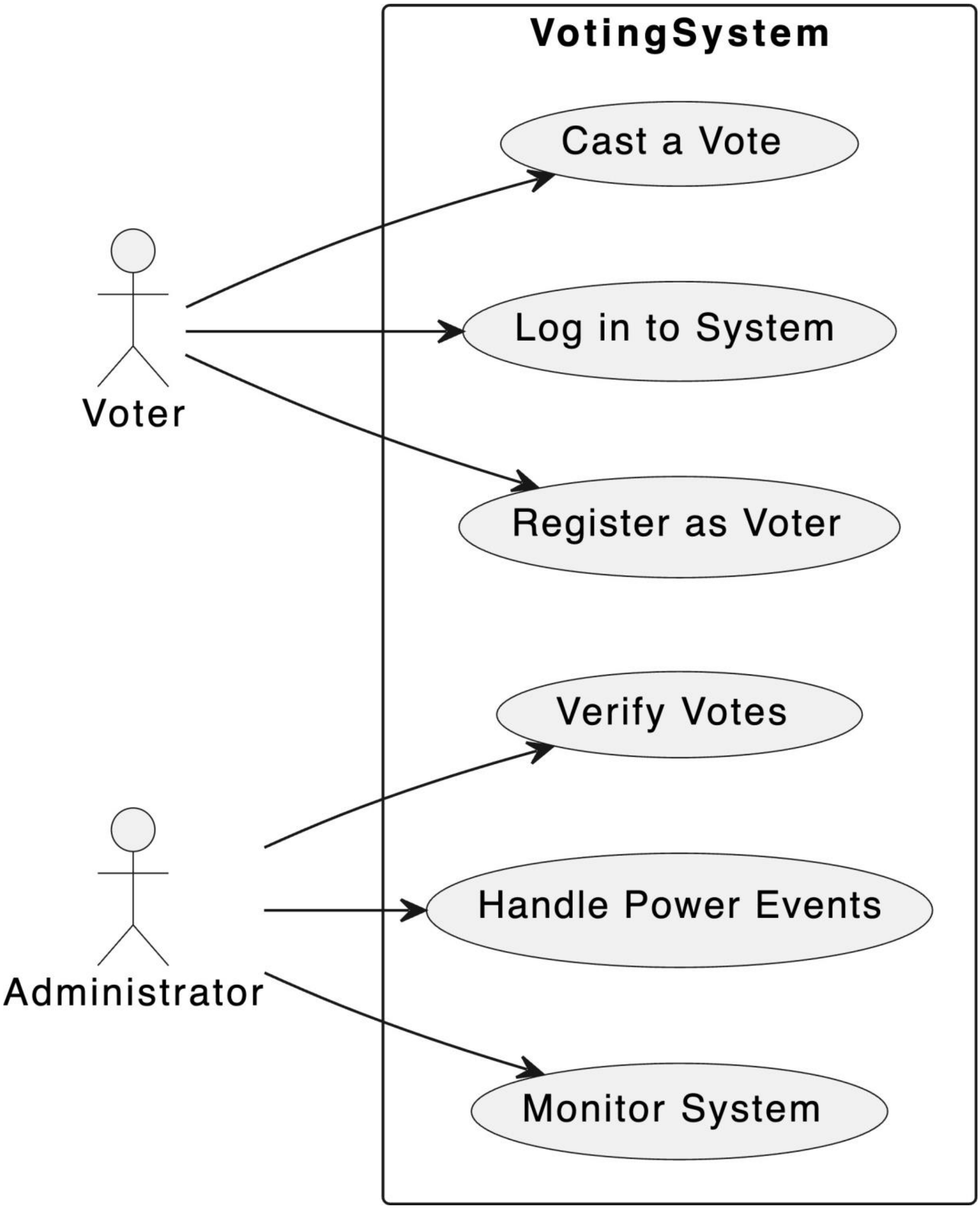

Figure 3.2 – Use Case Diagram of the Proposed System

The use case diagram (Figure 3.2) provides an overview of the interactions between actors (Voter and Administrator) and the system. It highlights the primary functionalities and their respective users.

3.4.3 Data Flow

1. **User Actions:** Voters register, authenticate, and cast ballots through the frontend.
2. **Backend Processing:** The backend validates user actions and interacts with the blockchain for secure data storage.
3. **Blockchain Operations:** Votes are recorded immutably, ensuring transparency and integrity.
4. **Offline Synchronization:** Data from offline voting is synchronized to the blockchain once connectivity is restored.

Database Design

- **Entities and Relationships**:
  - **Voter**:
    - Attributes: voterID (Primary Key), name, email, password.
    - Relationships: Casts votes (one-to-many relationship with Vote).
  - **Vote**:
    - Attributes: voteID (Primary Key), candidateID, voterID (Foreign Key), timestamp.
    - Relationships: Linked to Voter and Candidate.
  - **Candidate**:
    - Attributes: candidateID (Primary Key), name, party.
    - Relationships: Receives votes (one-to-many relationship with Vote).
  - **PowerEvent**:
    - Attributes: eventID (Primary Key), timestamp, status, description.

- Relationships: Triggers backup actions (one-to-one relationship with Backup).

- **Backup**:
  - Attributes: backupID (Primary Key), filePath, timestamp.
  - Relationships: Linked to PowerEvent.

Relationships:

1. A **Voter** can cast multiple **Votes**.
2. Each **Vote** is associated with one **Candidate**.
3. A **PowerEvent** can trigger a single **Backup**, ensuring data integrity during disruptions.

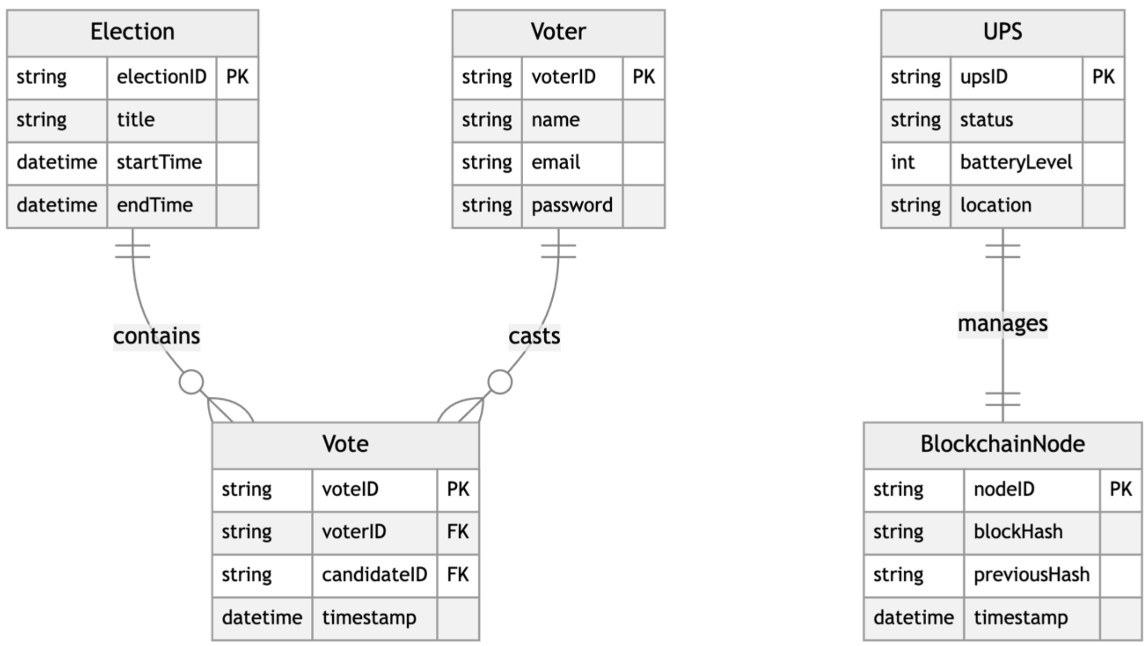

Figure 3.3 – Entity Relationship Diagram of the Proposed System

The database design is represented using an Entity Relationship Diagram (ERD) to visualize the relationships between key entities such as voters, votes, and power events (Figure 3.3).

3.5 System Design Overview

The system design encompasses the architecture, data flow, and module interactions to ensure robust performance and reliability.

Design Principles

1. **Modularity:** The system is divided into discrete components (e.g., voter module, administrator module) to simplify development and maintenance.
2. **Scalability:** The architecture supports growth in user base and data volume without performance degradation.
3. **Security:** Data encryption, secure authentication, and blockchain integration ensure the confidentiality and integrity of electoral data.
4. **Resilience:** The system is designed to handle power outages and connectivity issues, ensuring uninterrupted operations.

3.5.1 Activity Diagram

The activity diagram visually distinguishes between Voter and Administrator workflows, emphasizing decision points and system interactions. It highlights the seamless integration of user actions, power monitoring, and data preservation processes, ensuring system reliability and security. It highlights decision points such as successful validation of voter details, vote encryption, and power status checks. It visually maps the flow of actions from start to finish, ensuring clarity in how the system handles critical events like voting and backup processes. Key activities include:

Voter Actions:

1. **Voter Registration**:
   - Voter provides registration details (name, email, password).
   - System validates and stores voter data in the database.
2. **Casting a Vote**:
   - Voter logs in to the system.
   - Voter selects a candidate and submits the vote.
   - System encrypts and stores the vote on the blockchain.

Administrator Actions:

1. **Admin Monitoring**:
   - Administrator logs in to monitor system activity.
   - Admin reviews power event logs and voting statistics.
2. **Power Monitoring and Backup**:
   - System detects power status changes using sensors.
   - In the event of a power disruption, the system triggers a backup process.
   - Backup data is stored on external storage and synchronized upon power restoration.

Decision Points and Flow:

- Validation of voter registration details.

- Successful login for both Voter and Administrator.
- Power disruption detection leading to backup initiation.
- Synchronization of data after power restoration.

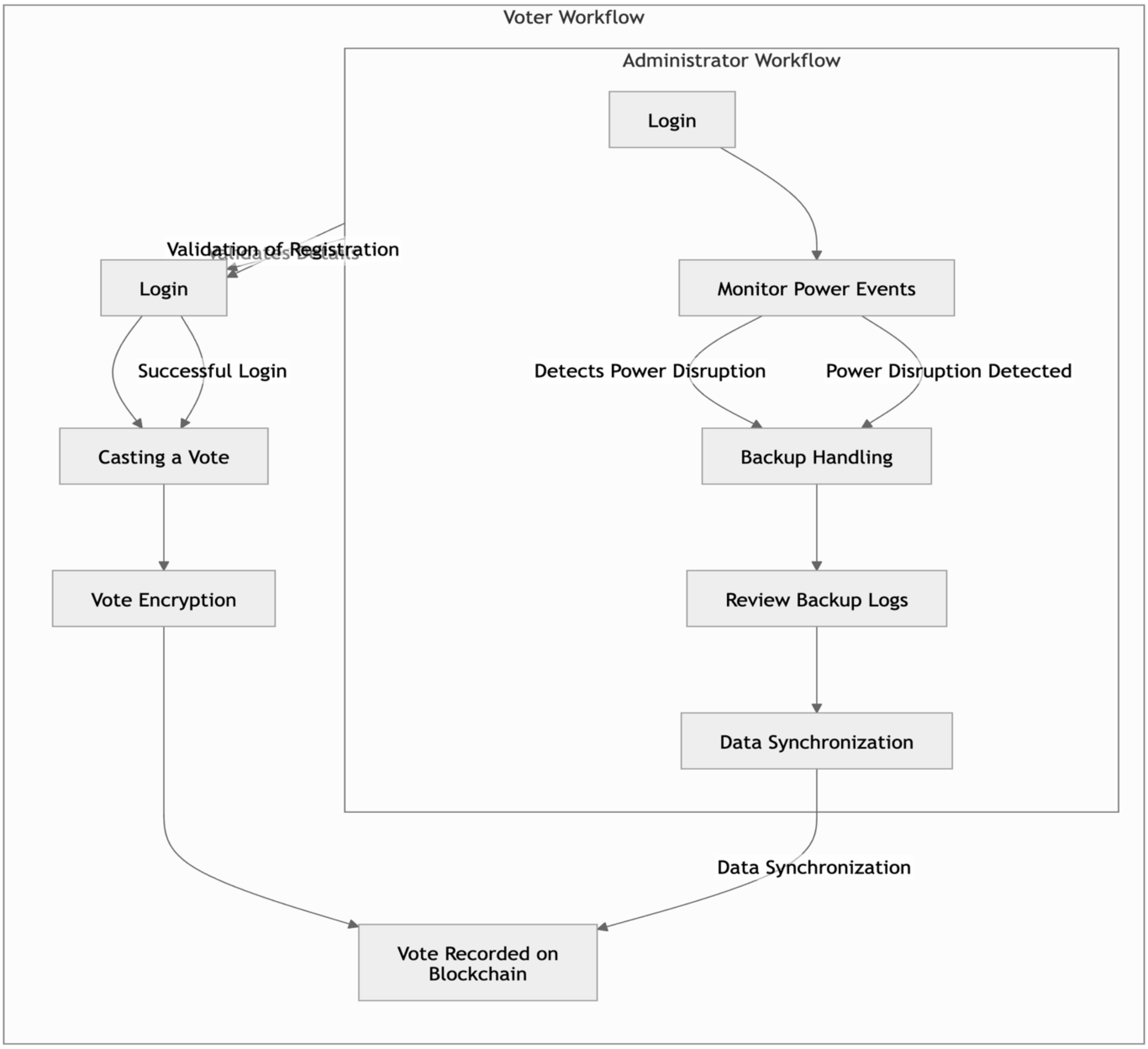

Figure 3.4 – Activity Diagram of the Proposed System

The activity diagram (Figure 3.4) outlines the workflow for key processes such as voting, power monitoring, and data synchronization, highlighting decision points and system interactions.

3.5.2 Class Diagram

Classes:

- **Voter**:
  - **Attributes**: voterID, name, email, password.
  - **Methods**: register(), login(), castVote().
- **Administrator**:
  - **Attributes**: adminID, name, email, password.
  - **Methods**: manageElections(), verifyVotes(), generateReports().
- **Vote**:
  - **Attributes**: voteID, voterID, candidateID, timestamp.
  - **Methods**: recordVote(), encryptVote().
- **PowerEvent**:
  - **Attributes**: eventID, timestamp, status, description.
  - **Methods**: logEvent(), notifyAdministrator().
- **BackupManager**:
  - **Attributes**: backupID, filePath, timestamp.
  - **Methods**: createBackup(), restoreBackup(), syncData().

Relationships:

1. **Voter to Vote**: A one-to-many relationship where a voter can cast multiple votes during different elections.
2. **Administrator to Vote**: A one-to-many relationship where an administrator manages and verifies multiple votes.

3. **Vote to Blockchain**: Association where votes are securely recorded and verified on the blockchain.
4. **PowerEvent to BackupManager**: A dependency relationship where power events trigger backup actions.
5. **Administrator to PowerEvent**: Administrators are notified of power events for auditing and resolution

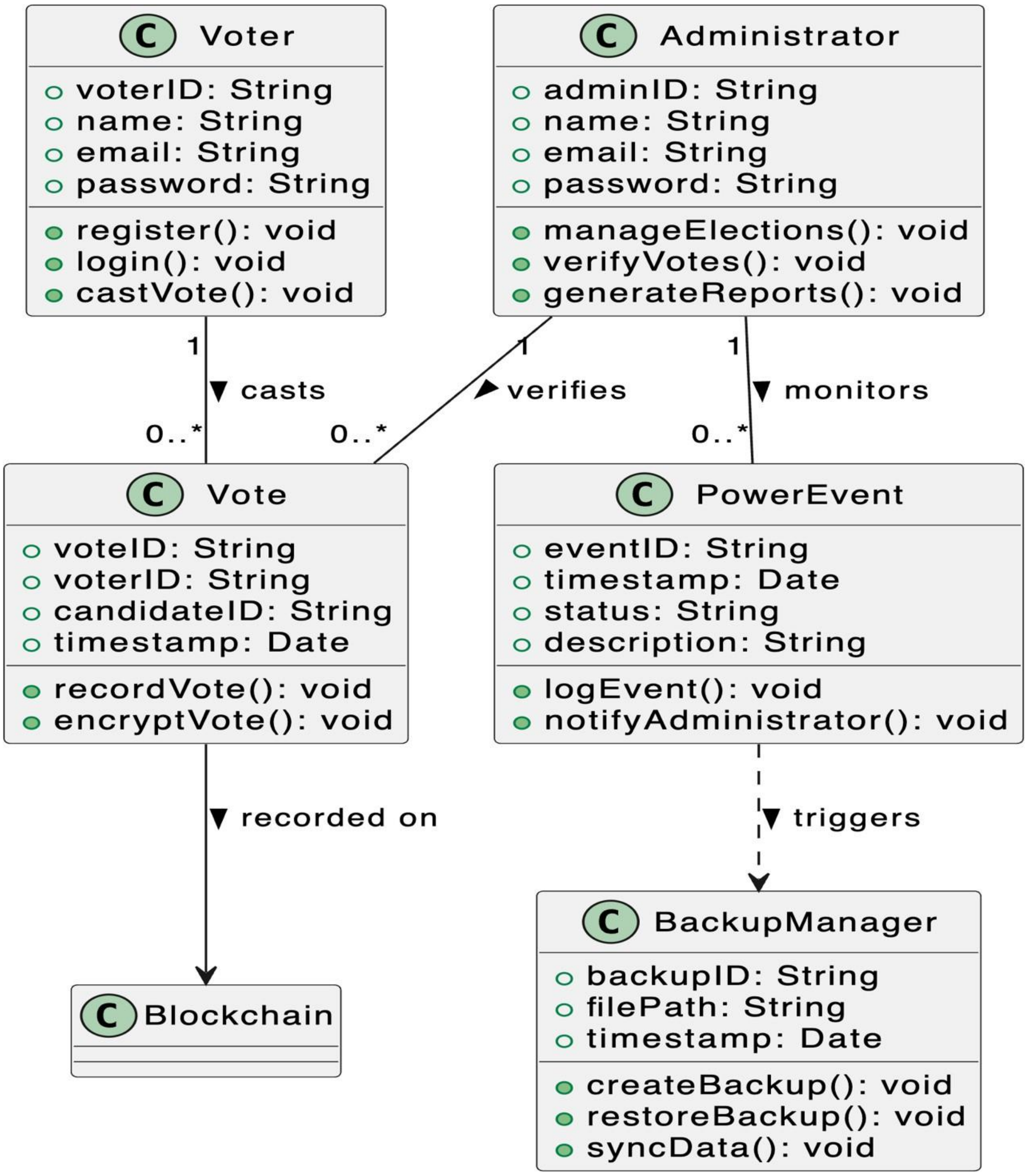

Figure 3.5 – Class Diagram of the Proposed System

The class diagram (Figure 3.5) illustrates the system's key classes, including their attributes and relationships. Key classes include Voter, Election, Vote, PowerEvent, and BackupManager.

REFERENCES

[1] MD. I. Khan et al., "Using Blockchain Technology for File Synchronization," *IOP Conf. Ser.*: Mater. Sci. Eng., vol. 561, 2019.

[2] D. Kumar, D. V. Chandini, and D. Reddy, "Secure Electronic Voting System Using Blockchain Technology," *Int. J. Smart Home*, vol. 14, no. 2, pp. 31-38, 2020.

[3] A. Rawat, V. Daza, and M. Signorini, "Offline Scaling of IoT Devices in IOTA Blockchain," *Sensors*, vol. 22, no. 1411, 2022.

[4] M. Ray et al., "Electronic Voting System Powered by Blockchain Technology: A Study," SSRN, 2023.

[5] CH. Sunandini et al., "A Framework to Make Voting System Transparent Using Blockchain Technology," 2020.

[6] S. Alagi et al., "Survey on Online E-voting System Using Blockchain Technology," IJARIIE, vol. 9, 2023.

[7] U. Jafar, M. J. Ab Aziz, Z. Shukur, and H. A. Hussain, "A Systematic Literature Review and Meta-Analysis on Scalable Blockchain-Based Electronic Voting Systems," *Sensors*, vol. 22, no. 7585, Oct. 2022. DOI: 10.3390/s22197585.

[8] F. S. Hardwick, A. Gioulis, R. N. Akram, and K. Markantonakis, "E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy," *Royal Holloway, Univ. of London*, 2016.

[9] F. Brandt and T. Sandholm, "Decentralized Voting with Unconditional Privacy," *AAMAS'05,* July 2005. DOI: 10.1145/1082473.1082524.

[10] R. Taş and Ö. Ö. Tanrıöver, "A Systematic Review of Challenges and Opportunities of Blockchain for E-Voting," *Symmetry*, vol. 12, no. 8, p. 1328, Aug. 2020

[11] A. Alshehri et al., "Privacy-Preserving E-Voting System Supporting Score Voting Using Blockchain," *Applied Sciences*, vol. 13, no. 2, p. 1096, Jan. 2023.

[12] J. Chai, "Blockchain-Based Voting System with Ethereum Blockchain," *Thesis*, The Ohio State University, 2020

[13] E. Rajathi et al., "Trustworthy Electronic Voting Using Adjusted Blockchain," *IJATEM*, 2023

[14] P. Shiwal et al., "Decentralized E-Voting System Using Blockchain," *IJNRD*, vol. 8, no. 5, 2023

[15] Jafar, U., Aziz, M. J. A., & Shukur, Z. "Blockchain for Electronic Voting System—Review and Open Research Challenges," *Sensors*, vol. 21, no. 5874, 2021. DOI: 10.3390/s21175874.

[16] Denis González, C., Frias Mena, D., Massó Muñoz, A., Rojas, O., & Sosa-Gómez, G. "Electronic Voting System Using an Enterprise Blockchain," *Applied Sciences*, vol. 12, no. 531, 2022. DOI: 10.3390/app12020531.

[17] Fusco, F., Lunesu, M. I., Pani, F. E., & Pinna, A. "Crypto-voting: A Blockchain-Based E-Voting System," in *Proc. 10th Int'l Conf. Knowledge Management & Information Sharing (KMIS)*, 2018, pp. 223–227. DOI: 10.5220/0006962102230227.

[18] A. K. Koç, E. Yavuz, U. C. Çabuk, and G. Dalkılıç, "Towards Secure E-Voting Using Ethereum Blockchain," IEEE, 2018. DOI: 10.1109/ISDFS.2018.8355340.

[19] L. Reddick, "Decentralized Voting: Ethereum-Based Voting Platform," 2018.

[20] M. Lamsani, S. Jatmiko, and F. Fadli, “Electronic Voting Using Decentralized System Based on Ethereum Blockchain,” *Jurnal Ilmiah Komputasi*, vol. 19, 2020. DOI: 10.32409/jikstik.19.1.152.

[21] C.-H. Roh and I.-Y. Lee, “A Study on Electronic Voting System Using Private Blockchain,” *J. Inf. Process Syst.*, 2020.

[22] D. Raikar and A. Vatsa, “BCT-Voting: A Blockchain Technology Based Voting System,” *Conf. Paper*, 2021

[23] U. C. Çabuk, E. Adıgüzel, and E. Karaarslan, “A Survey on Feasibility and Suitability of Blockchain Techniques for E-Voting Systems,” *IJARCCE*, 2018.

[24] A. Yadav et al., "E-Voting Using Blockchain Technology," IJERT, 2020

[25] A. Lahane et al., "Blockchain Technology-Based E-Voting System," ITM Conf., 2020.

[26] A. Benny et al., "Blockchain-Based E-Voting System," SSRN, 2020.

[27] Peelam, M.S., Kumar, G., et al. "DemocracyGuard: Blockchain-Based Secure Voting Framework," *Expert Systems*, 2024.

[28] Isirova, K., Kiian, A., et al. "Decentralized Electronic Voting System Based on Blockchain Technology," *CMIS Proceedings*, 2020.

[29] B. Shahzad and J. Crowcroft, “Trustworthy Electronic Voting Using Adjusted Blockchain Technology,” *IEEE Access*, vol. 7, 2019.

[30] Md. S. Arnob et al., “Blockchain-Based Secured E-Voting System,” *International Research Journal of Engineering and Technology*, vol. 7, no. 1, 2020.

[31] M. Pathak et al., “Blockchain-Based E-Voting System,” *International Journal of Scientific Research in Science and Technology*, vol. 8, no. 3, 2021.