DECENTRALIZED E-VOTING SYSTEM leveraging the NANO blockchain

Innovative Project 3 (PRJCS581)

Submitted

In partial fulfillment for the Degree of

Bachelor of Technology

In

Department of CSE(IoT)

Submitted by

Utsav Sarda

Enrolment no: 12022002019058

Under the Guidance of

Prof. Swagatam Basu

IEM

श्रद्धावान लभते ज्ञानम्

INSTITUTE OF ENGINEERING & MANAGEMENT

Good Education, Good Jobs

Institute of Engineering and Management
Kolkata
November, 2024

Index Page

Acknowledgement

I wish to express my heartfelt gratitude to all the people who have played a crucial role in the research for this project, without their active cooperation the preparation of this project could not have been completed within the specified time limit. I am thankful to my Project Guide ***Prof. Swagatam Basu*** who supported me throughout this project with utmost cooperation and patience and for helping me in doing this Project.

I am also thankful to our respected Head of the Department, ***Prof. Dr. Moutushi Singh***, for motivating me to complete this project with complete focus and attention.

I am thankful to my department and all my teachers for the help and guidance provided for this work.

I extend my sincere thanks to my institute, the Institute of Engineering and Management, Kolkata for the opportunity provided to me for the betterment of my academics.

Utsav Sarda
Department of CSE(Iot)
Enrolment No:
12022002019058
Date: 20/11/2024
Place: Kolkata

ABSTRACT

Voting, a very integral core of democratic societies, allows citizens to express their choices and shape policies for their good governance. It is an essential right and a critical mechanism for ensuring representation, accountability, and fairness in decision-making processes. For decades, the traditional method of voting has been paper ballots followed by electronic means in a bid to enable greater accessibility, efficiency, and accuracy. However, these system arrangements have always suffered from security vulnerabilities, high costs, and fraud or manipulation risks. The digital age exposes the need for a more reliable, transparent, and accessible voting system. Decentralized technologies, such as blockchain, offer a transformative approach to meet these challenges through fostering trust and inclusiveness, which at the same time protect the integrity of the electoral process. Decentralized voting systems make sure safe, transparent, and impenetrable elections by applying blockchain technology. This project offers a decentralized electronic voting mechanism, using Nano, a feeless transaction platform with low energy efficiency, renowned for quick block lattice architecture. In this system, eliminating middlemen is performed by using Nano's special capabilities to provide end-to-end trust and instant vote validation. Every voter is assigned a unique cryptographic identifier; once cast, it is then saved as an immutable transaction on the Nano network. This technique retains voter identity and keeps transparency while minimizing the risks of fraud, illegal access, and vote tampering. The system is available worldwide with little infrastructure needed, scalable, and can accommodate high throughput during peak voting hours. Coupled with modern cryptographic techniques and Nano's advanced consensus mechanism, this system provides a robust solution for conducting free and fair elections in a digital age.

PROBLEM DEFINITION

Traditional voting systems, both paper and electronic types of systems, exhibit several critical challenges that lead to the deterioration of integrity, accessibility, and efficiency in the electoral process. They easily fall into risks like vote tampering, fraud, as well as unauthorized access, leading to compromised accuracy in the election results. Additionally, in most cases, voters lack transparency in where votes are recorded and counted. Centralized voting systems are also vulnerable to single points of failure, which makes them easy prey for cyberattacks and outages.

Moreover, voter anonymity coupled with the verifiability and auditability of the election process still poses significant challenges. In this era of digital transformation, there is a definite need for a voting system that is both secure and transparent, scalable, and accessible to all voters irrespective of the location.

This project solves these problems by proposing the decentralized voting system through application of the blockchain technology of Nano to guarantee trust, integrity, and efficiency in elections.

INTRODUCTION

In today's digital age, the need for secure, transparent, and efficient voting systems has become more critical than ever. Traditional voting methods often face challenges like logistical inefficiencies, susceptibility to fraud, and lack of transparency. To address these challenges, the integration of blockchain technology into voting systems is emerging as a promising solution.

This project aims to develop an **e-voting system leveraging the Nano blockchain**, a decentralized, fast, and energy-efficient cryptocurrency platform. Nano's unique features, such as feeless transactions, minimal resource consumption, and high scalability, make it an ideal choice for implementing a modern, blockchain-based e-voting mechanism.

Nano employs a unique **block-lattice structure**, a groundbreaking innovation in blockchain technology, to achieve high scalability, low latency, and feeless transactions. Unlike traditional blockchains that rely on a single chain where all transactions are processed sequentially, Nano's block-lattice introduces a more efficient and decentralized approach.

The proposed system ensures:

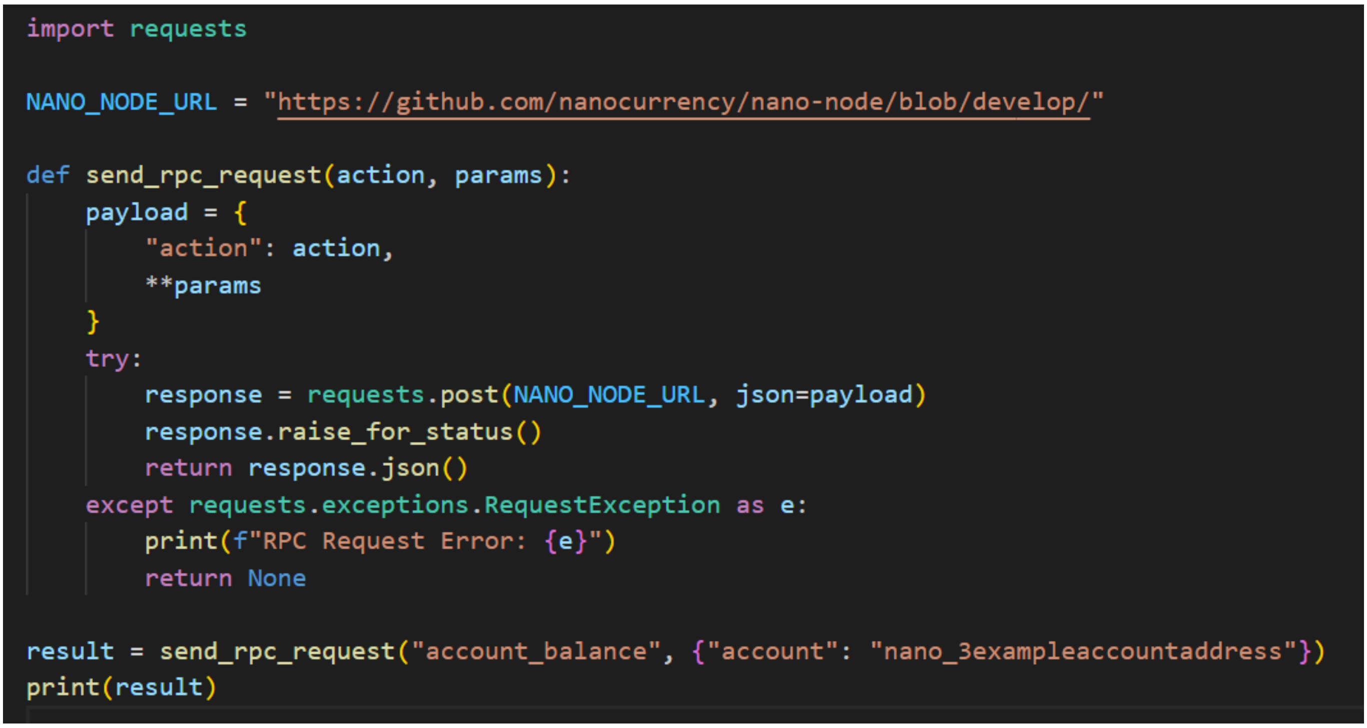
- **Security**: Votes are cryptographically secured and immutable.
- **Transparency**: The entire voting process is auditable on the blockchain.
- **Accessibility**: Voters can cast their votes remotely using a secure interface.
- **Efficiency**: The system eliminates delays in vote counting with real-time updates.

This project not only demonstrates the potential of Nano blockchain technology in solving real-world problems but also serves as a foundation for secure, decentralized voting applications in various domains, including corporate governance, community decisions, and public elections.

WORK DONE

1. NANO_NODE API INTEGRATION VIA RPC:-

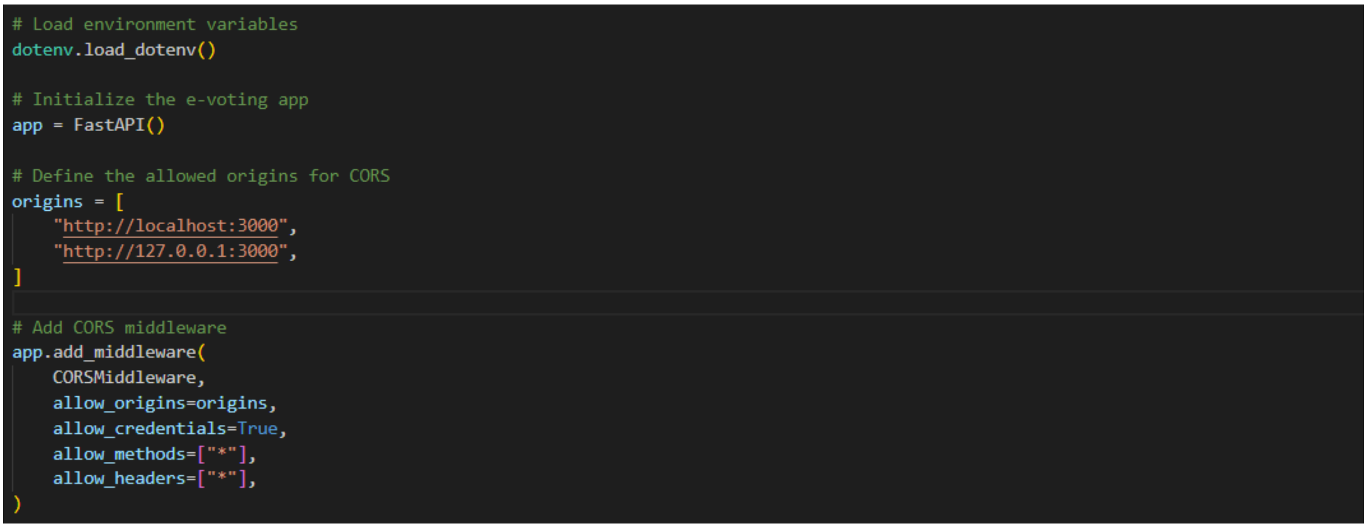
Instead of a Python library, HTTP requests are used to interact with a Nano node. Below is an example of how a request is sent:-



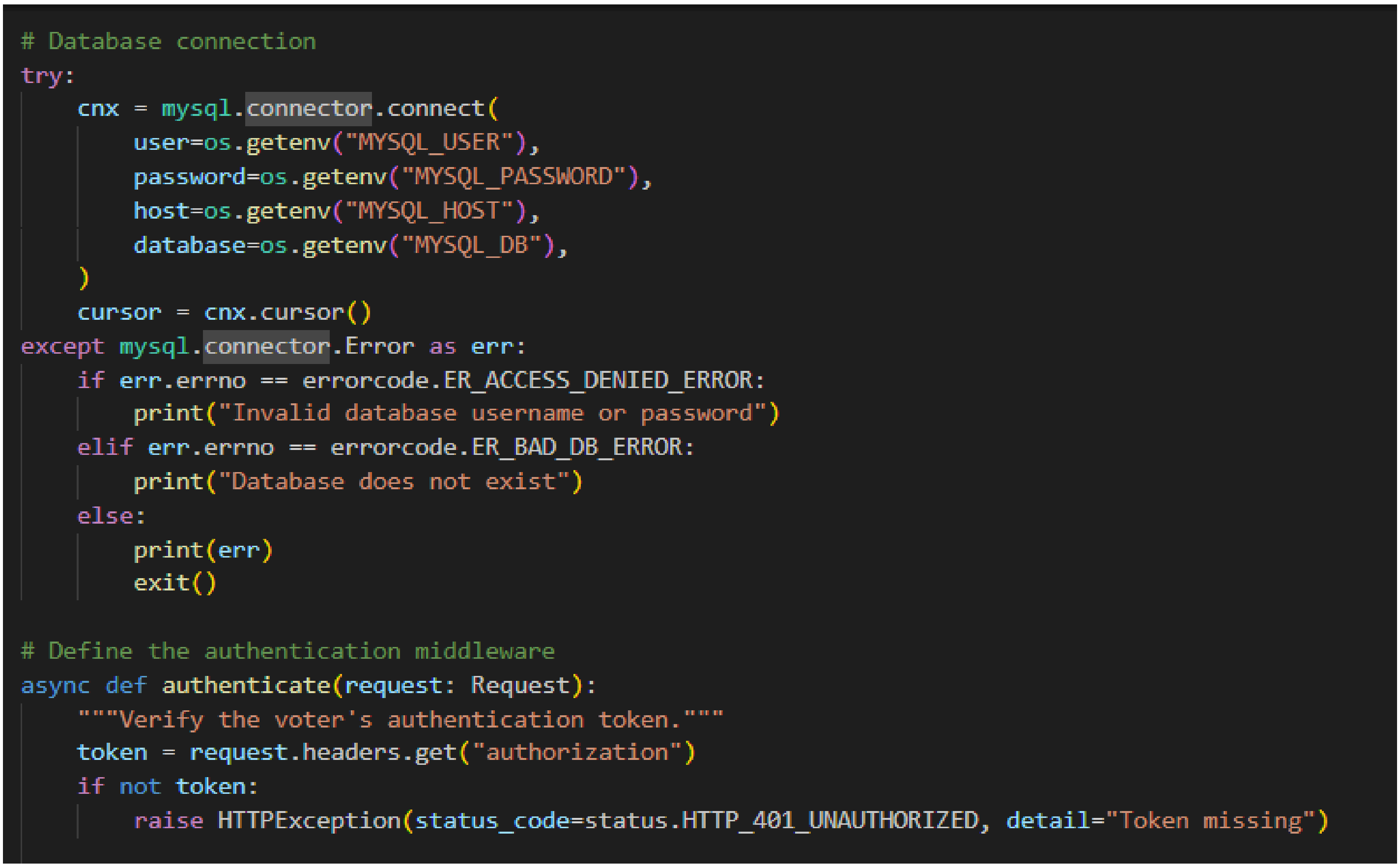
```python
import requests

NANO_NODE_URL = "https://github.com/nanocurrency/nano-node/blob/develop/"

def send_rpc_request(action, params):
    payload = {
        "action": action,
        **params
    }
    try:
        response = requests.post(NANO_NODE_URL, json=payload)
        response.raise_for_status()
        return response.json()
    except requests.exceptions.RequestException as e:
        print(f"RPC Request Error: {e}")
        return None

result = send_rpc_request("account_balance", {"account": "nano_3exampleaccountaddress"})
print(result)
```

2. MySQL Database Integration:-

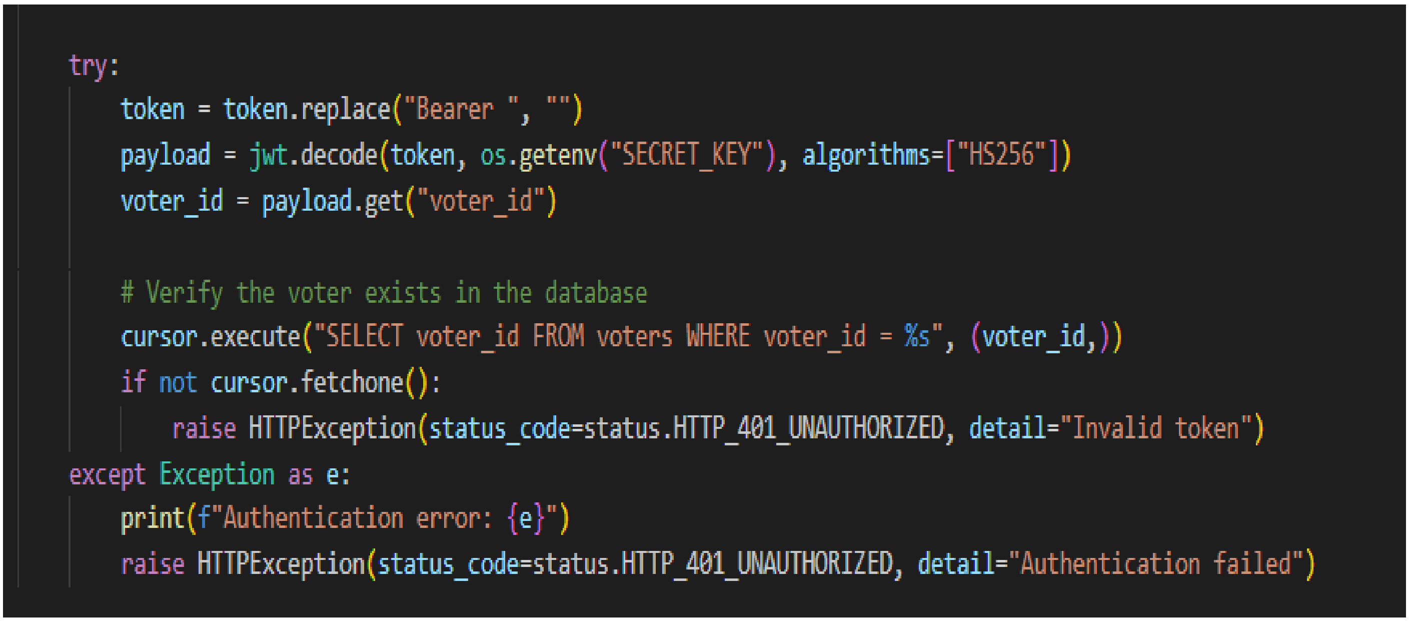
MySQL Database is integrated to check the validity of the Voters and ensure only registered users are allowed to vote. The py integration is done as:-



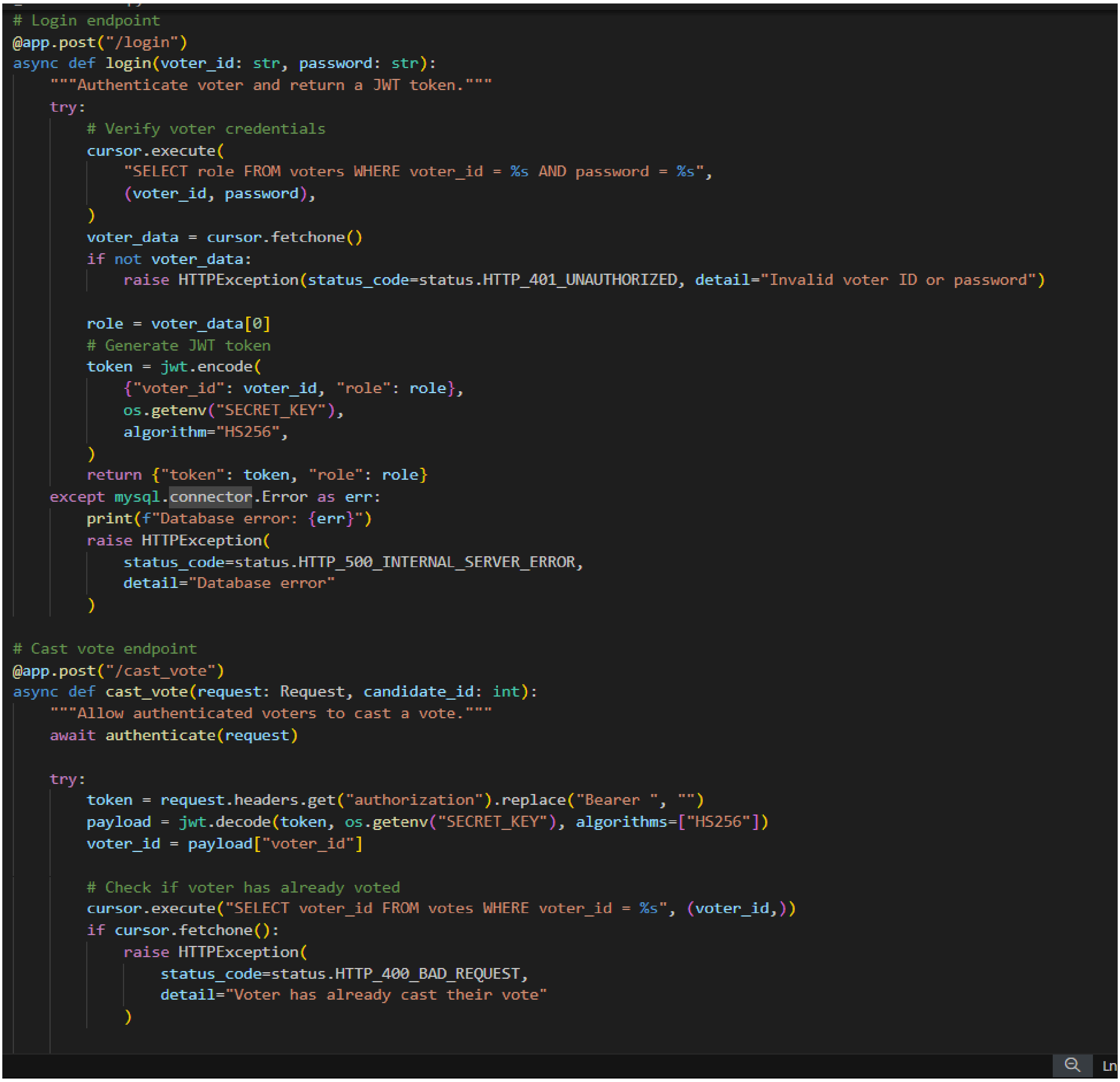
```python
# Load environment variables
dotenv.load_dotenv()

# Initialize the e-voting app
app = FastAPI()

# Define the allowed origins for CORS
origins = [
    "http://localhost:3000",
    "http://127.0.0.1:3000",
]

# Add CORS middleware
app.add_middleware(
    CORSMiddleware,
    allow_origins=origins,
    allow_credentials=True,
    allow_methods=["*"],
    allow_headers=["*"],
)
```



```
# Database connection
try:
    cnx = mysql.connector.connect(
        user=os.getenv("MYSQL_USER"),
        password=os.getenv("MYSQL_PASSWORD"),
        host=os.getenv("MYSQL_HOST"),
        database=os.getenv("MYSQL_DB"),
    )
    cursor = cnx.cursor()
except mysql.connector.Error as err:
    if err.errno == errorcode.ER_ACCESS_DENIED_ERROR:
        print("Invalid database username or password")
    elif err.errno == errorcode.ER_BAD_DB_ERROR:
        print("Database does not exist")
    else:
        print(err)
        exit()

# Define the authentication middleware
async def authenticate(request: Request):
    """Verify the voter's authentication token."""
    token = request.headers.get("authorization")
    if not token:
        raise HTTPException(status_code=status.HTTP_401_UNAUTHORIZED, detail="Token missing")
```



```
    try:
        token = token.replace("Bearer ", "")
        payload = jwt.decode(token, os.getenv("SECRET_KEY"), algorithms=["HS256"])
        voter_id = payload.get("voter_id")

        # Verify the voter exists in the database
        cursor.execute("SELECT voter_id FROM voters WHERE voter_id = %s", (voter_id,))
        if not cursor.fetchone():
            raise HTTPException(status_code=status.HTTP_401_UNAUTHORIZED, detail="Invalid token")
    except Exception as e:
        print(f"Authentication error: {e}")
        raise HTTPException(status_code=status.HTTP_401_UNAUTHORIZED, detail="Authentication failed")
```



```python
# Login endpoint
@app.post("/login")
async def login(voter_id: str, password: str):
    """Authenticate voter and return a JWT token."""
    try:
        # Verify voter credentials
        cursor.execute(
            "SELECT role FROM voters WHERE voter_id = %s AND password = %s",
            (voter_id, password),
        )
        voter_data = cursor.fetchone()
        if not voter_data:
            raise HTTPException(status_code=status.HTTP_401_UNAUTHORIZED, detail="Invalid voter ID or password")

        role = voter_data[0]
        # Generate JWT token
        token = jwt.encode(
            {"voter_id": voter_id, "role": role},
            os.getenv("SECRET_KEY"),
            algorithm="HS256",
        )
        return {"token": token, "role": role}
    except mysql.connector.Error as err:
        print(f"Database error: {err}")
        raise HTTPException(
            status_code=status.HTTP_500_INTERNAL_SERVER_ERROR,
            detail="Database error"
        )

# Cast vote endpoint
@app.post("/cast_vote")
async def cast_vote(request: Request, candidate_id: int):
    """Allow authenticated voters to cast a vote."""
    await authenticate(request)

    try:
        token = request.headers.get("authorization").replace("Bearer ", "")
        payload = jwt.decode(token, os.getenv("SECRET_KEY"), algorithms=["HS256"])
        voter_id = payload["voter_id"]

        # Check if voter has already voted
        cursor.execute("SELECT voter_id FROM votes WHERE voter_id = %s", (voter_id,))
        if cursor.fetchone():
            raise HTTPException(
                status_code=status.HTTP_400_BAD_REQUEST,
                detail="Voter has already cast their vote"
            )
```

3.Website Development:-

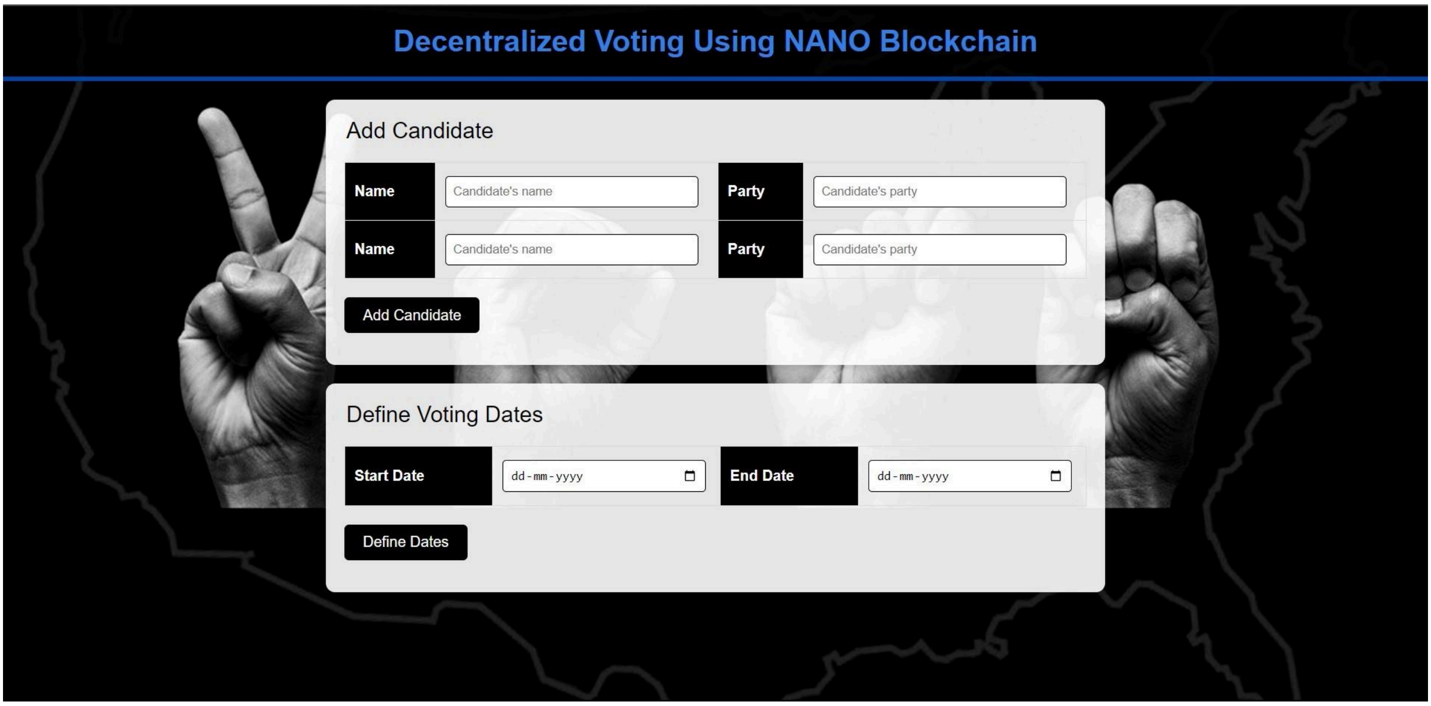
a. ADMIN PAGE

The website serves a simple and user-friendly layout. It takes two basic data inputs from the admin-

•Candidate Information: Names of the candidates competing in the elections along with their party name.

•Election Date: A specific timeline in which the users can cast their votes.

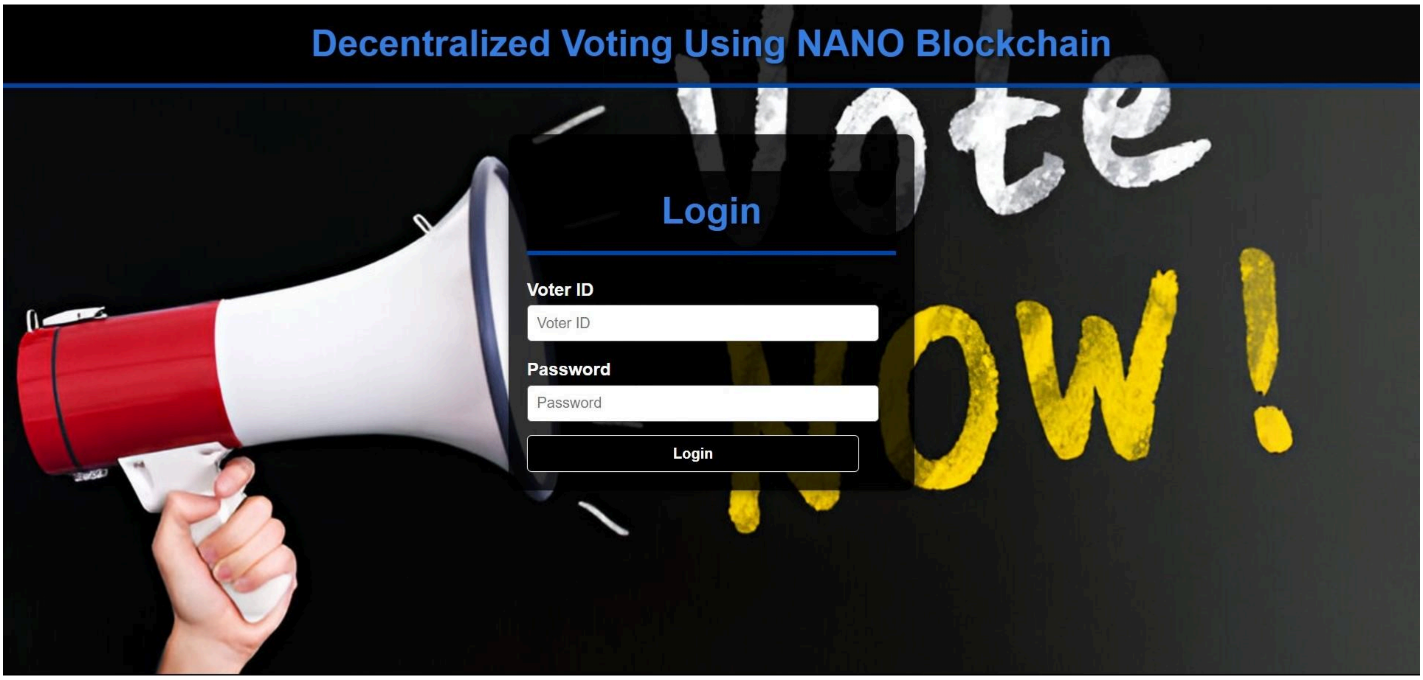
These specifications would then be visible to the voters, who can securely cast their votes at their own preferred times.



b. LOGIN PAGE

A simple and secure login page allows the user to enter their respective accounts to cast their votes.

Such individual-based login IDs also ensure that only one vote is being cast by one person



REVIEW OF RELATED WORK

A Comparative Review of Ethereum and Solana-Based E-Voting Systems

Ethereum-Based E-Voting Systems

Strengths:

- Smart Contract Transparency: Leveraging Ethereum's smart contracts ensures immutable and transparent vote recording.
- Diverse Authentication Methods: Supports various authentication mechanisms, including blockchain wallets, facial recognition, and OTPs.
- Decentralized Trust: Some implementations prioritize decentralization by minimizing reliance on centralized entities.

Weaknesses:

- High Transaction Costs: Ethereum's gas fees can be prohibitive, especially for large-scale elections.
- Scalability Limitations: The network's capacity to handle a high volume of concurrent votes can be constrained.
- Privacy Concerns: Storing voter identifiers on-chain poses risks to privacy and anonymity.
- Centralization Risks: Reliance on external systems (e.g., OTP servers) can compromise decentralization.
- Energy Consumption: While Ethereum has transitioned to Proof of Stake, energy consumption remains a concern.

Solana-Based E-Voting Systems

Strengths:

- High Throughput and Low Fees: Solana's high throughput and low transaction costs make it suitable for e-voting.
- Fast Transaction Validation: Proof of History (PoH) consensus mechanism ensures rapid transaction finality.
- Performance-Optimized Smart Contracts: Solana's smart contracts are designed for efficiency, reducing latency in vote tallying and recording.

Weaknesses:

- Centralization Risks: Solana's validator ecosystem is less decentralized compared to other blockchains.
- Network Outages: Historical instances of network downtime raise concerns about system reliability.
- Complex Development: Rust and C programming languages used for Solana smart contracts can be challenging for developers.
- Data Storage Limitations: Solana's design prioritizes lightweight data storage, limiting the scope of on-chain voter or election metadata.

Common Challenges in Both Systems

- Voter Privacy: Both systems face challenges in ensuring complete voter anonymity while maintaining accountability.
- Internet Dependency: Online-only access limits participation in regions with poor internet connectivity.
- Single Points of Failure: Reliance on third-party servers for verification or data storage introduces vulnerabilities.
- User Experience: Technical barriers, such as wallet setup and key management, can hinder user adoption.

While Ethereum and Solana offer promising foundations for blockchain-based e-voting systems, significant challenges remain. High costs, privacy concerns, scalability issues, and user experience barriers hinder widespread adoption. A hybrid approach, combining blockchain technology with privacy-preserving techniques and user-centric design, is necessary to build robust and secure e-voting systems.

REMAINING WORK TO BE ACCOMPLISHED

1. Wallet Generation and User Onboarding

- Unique Nano Wallet Creation: Generate a unique Nano wallet for each registered user to serve as their digital identity within the voting system.
- Wallet Security: Implement robust security measures to protect user wallets from unauthorized access, ensuring the integrity of their votes.
- User-Friendly Interface: Design an intuitive interface that guides users through the wallet creation process, making it accessible to a wide range of users.

2. Secure and Private Voting

- Vote Encryption: Employ strong encryption algorithms to encrypt each vote before it's recorded on the Nano blockchain.
- Anonymization Techniques: Implement advanced anonymization techniques, such as zero-knowledge proofs, to conceal voter identities while maintaining the integrity of the voting process.
- Blockchain Immutability: Leverage the blockchain's immutable nature to ensure that once votes are recorded, they cannot be altered or tampered with.

3. Biometric Authentication for Enhanced Security

- Biometric Data Collection: Collect biometric data (e.g., fingerprints, facial recognition) from registered users to verify their identities.
- Secure Storage: Store biometric data securely, using encryption and other security measures to prevent unauthorized access.
- Real-time Verification: Integrate biometric authentication into the voting process to ensure that only authorized individuals can cast votes.

4. Centralized Node for Administration and Monitoring

- Principal Nano Node Setup: Establish a dedicated Nano node to serve as the central administrative hub for the voting system.
- Network Synchronization: Ensure seamless communication and

synchronization between the principal node and the Nano network to maintain data consistency.
- Security Protocols: Implement robust security protocols to protect the principal node from cyberattacks and unauthorized access.
- Real-time Monitoring: Monitor network activity, vote tallies, and potential security threats in real-time.

5. Transparent and Real-time Results

- Live Vote Tallying: Develop a system to continuously tally votes and display real-time results on the platform's homepage.
- Data Visualization: Use clear and concise data visualizations to present voting trends and outcomes.
- Security Considerations: Implement measures to prevent manipulation of live results and ensure the accuracy of the displayed information.
- Delayed Release of Final Results: Consider delaying the final release of results to allow for potential audits and dispute resolution.

CONCLUSION

To conclude, the overall development of this blockchain-based e-voting system has advanced, integrating the nodes made using Nano, admin interface, and login pages connected to MySQL database-all of which are essential components in making up the system. They will ensure secure and decentralized vote recording via the Nano blockchain, but users are also correctly authenticated through login pages.

With these foundational elements in place, the system is well-equipped to tackle the main issues of scalability, transparency, and security. Still, much work needs to be done to bring the project to its full completion. These include the processes of creating Nano wallets for all registered users so that voting is carried out securely, carrying out robust cryptographic measures that will protect the anonymity of the voter, and obtaining inclusion of biometric authentication for further security. The creation of a Principal Nano node for the admin will allow for the effective administration of the voting process, while a real-time vote results dashboard will offer transparency and live updates during elections.

The work done so far provides a robust platform for comprehensive and secure e-voting, and the tasks remaining will make sure that the platform meets standards set for privacy, usability, and efficiency.

REFERENCES

1. Nano Node Repository. (n.d.). Retrieved from https://github.com/nanocurrency/nano-node
2. Voter Authentication Using Biometric and Facial Recognition Systems. (2023). MDPI. Retrieved from https://www.mdpi.com/2813-5288/2/4/17#:~:text=To%20verify%20each%20voter's%20information,biometric%20and%20facial%20recognition%20systems
3. Nano Blockchain Integration Guide. (n.d.). Retrieved from https://docs.nano.org/integration-guides/the-basics/
4. Singh, S., & Kumar, V. (2020). Ethereum-based E-voting Systems: Challenges and Solutions. *International Journal of Computer Science and Information Security, 18*(6), 256-264.
5. Yousif, R., & Mohamad, H. (2022). Hybrid Blockchain Framework for Energy-Efficient and Scalable E-Voting Systems. *Journal of Blockchain Technology, 6*(2), 110-118.
6. Das, D., & Jain, P. (2021). Face Recognition and Blockchain for Secure E-Voting: A Novel Approach. *International Journal of Blockchain Applications, 3*(1), 45-55.
7. MetaMask Documentation. (n.d.). Retrieved from https://metamask.io/
8. Ethereum Documentation. (n.d.). Retrieved from https://ethereum.org/en/developers/docs/
9. Nano Community. (2023). *Nano: The Fast, Feeless Cryptocurrency*. Retrieved from https://nano.org/