REQUIREMENT ANALYSIS

Date	19 September 2022
Team ID	NM2023TMID02226
Project Name	CLIMATE TRACK SMART USING BLOCK CHAIN
Maximum Marks	4 Marks

FUNCTIONAL REQUIREMENT

Creating a climate tracking system using blockchain technology involves a combination of functional requirements that ensure the system's effectiveness and reliability. Here is a list of functional requirements for a climate tracking smart system using blockchain:

1. Data Collection and Integration:
   a. Real-time data collection from various sources, such as weather stations, satellites, IoT devices, and climate sensors.
   b. Integration of diverse data types, including temperature, humidity, air quality, carbon emissions, and more.

2. Data Validation and Accuracy:
   a. Implement data validation mechanisms to ensure the accuracy and reliability of the data.
   b. Incorporate consensus algorithms within the blockchain network to prevent data manipulation.

3. Blockchain Implementation:
   a. Choose an appropriate blockchain platform (e.g., Ethereum, Hyperledger) to build the system.
   b. Develop smart contracts for data recording, verification, and access control.

4. Decentralization and Security:
   a. Ensure a decentralized network of nodes to prevent a single point of failure.
   b. Implement strong encryption and cryptographic techniques to secure data and transactions.

5. User Authentication and Access Control:
   Implement user authentication and authorization mechanisms to control access to climate data.

OPERATIONAL REQUIREMENTS

Operational requirements for a climate tracking smart system using blockchain focus on how the system functions in a day-to-day context and how it meets the needs of its users. These requirements ensure that the system operates efficiently and effectively. Here are some operational requirements for such a system:

1. Data Ingestion and Collection:
   a. Regularly collect real-time climate data from various sources.
   b. Ensure data integrity and quality during the ingestion process.
   c. Establish automated data feeds and connections with data providers.

2. Data Processing and Validation:
   a. Implement real-time data validation to detect anomalies and errors.
   b. Ensure that collected data conforms to predefined standards.
   c. Incorporate data cleaning and preprocessing procedures.

3. Consensus Mechanisms:
   a. Choose an appropriate consensus algorithm (e.g., Proof of Work, Proof of Stake) for blockchain validation.
   b. Configure consensus parameters for network efficiency and security.

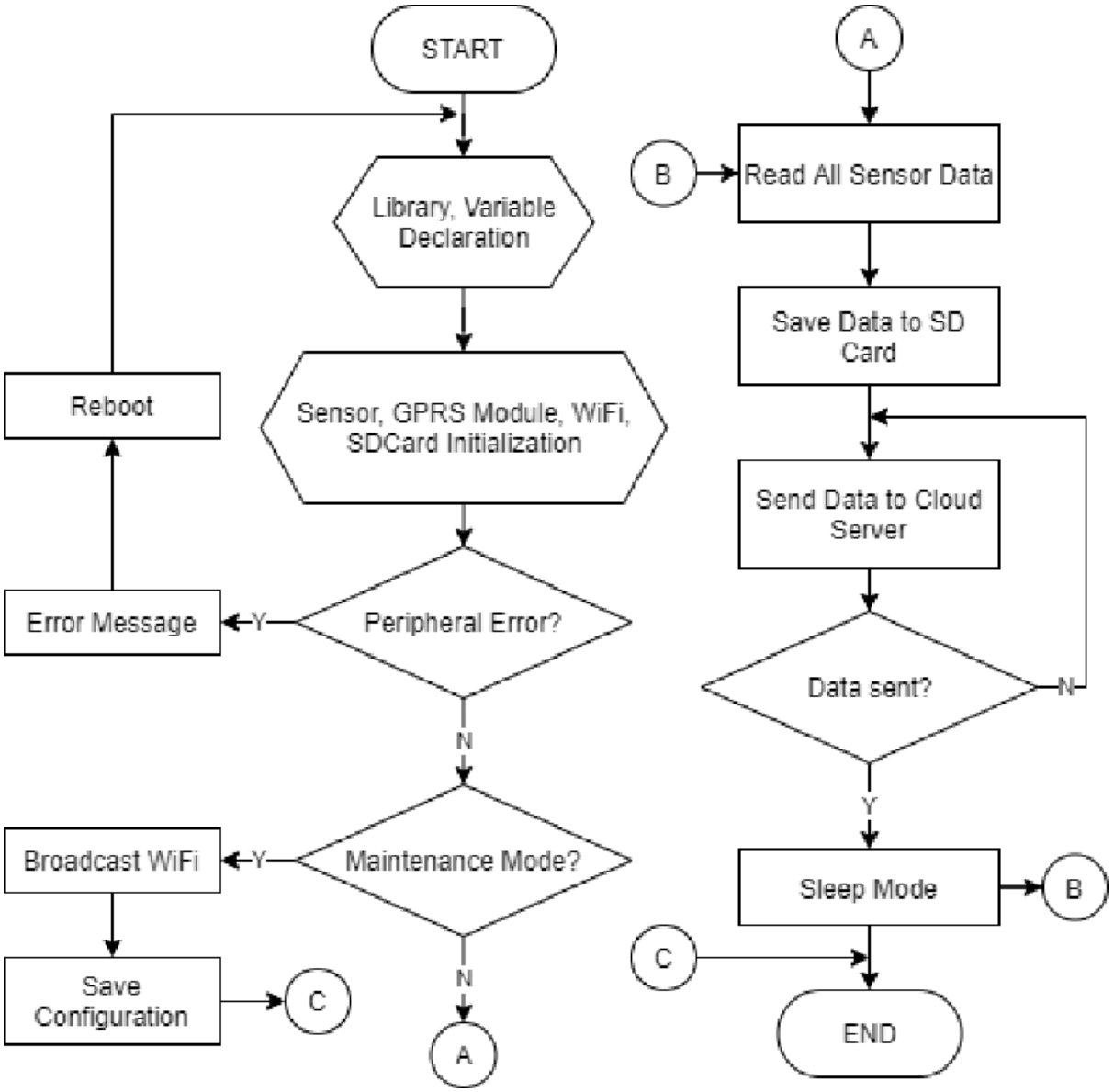
4. Blockchain Governance:
   a. Define a governance model to manage network upgrades, security patches, and rule changes.
   b. Establish a decision-making process for blockchain protocol changes.

5. Node Management:
   a. Maintain a network of distributed nodes to support decentralization.
   b. Monitor the health and performance of nodes to ensure network reliability.
   c. Implement mechanisms for adding and removing nodes as needed.

6. Security and Compliance:
   a. Regularly assess and update security measures to protect against threats and vulnerabilities.
   b. Ensure compliance with relevant data security regulations and privacy laws.

7. Data Access Control:
   a. Enforce access control policies to restrict data access based on user roles and permissions.
   b. Implement mechanisms for user authentication and authorization.

FLOW CHART


START
Library, Variable Declaration
Sensor, GPRS Module, WiFi, SDCard Initialization
Peripheral Error?
Y
Error Message
Reboot
N
Maintenance Mode?
Y
Broadcast WiFi
Save Configuration
C
N
A
A
B
Read All Sensor Data
Save Data to SD Card
Send Data to Cloud Server
Data sent?
N
Y
Sleep Mode
B
C
END