Birla Institute of Technology and Science-Pilani, Hyderabad Campus

---

Report

Healthcare Record Management System using Blockchain Technology

Tejasvini Goel- 2022A7PS1672H

Simran Sesha Rao- 2022A7PS0002H

Simran Singh- 2022A7PS0003H

Ruchi Harge- 2022B4A70942H

Under the supervision of

PROF. G GEETHAKUMARI

22st September, 2025

ABSTRACT

This report presents **MedChain**, a blockchain-based healthcare record management system designed to ensure the integrity, privacy, and authenticity of patient medical records. The platform supports user registration (patients, doctors, and administrators), record addition and updates, viewing of tamper-proof histories, and comprehensive operation logging. A **Delegated Proof-of-Stake (DPoS)** consensus mechanism ensures that only elected delegates can forge blocks, enhancing security and efficiency. **Merkle trees** provide cryptographic hashing of transaction data, enabling tamper-evident verification of records. The system maintains accountability through access logs and verifiable histories, effectively preventing unauthorized edits while supporting multi-user interactions. By combining blockchain immutability with a **patient consent workflow** and digital signatures, MedChain demonstrates a secure, auditable, and scalable solution for modern healthcare record management, showcasing reliable transaction recording, secure block creation, and verifiable history retrieval.

INTRODUCTION

In large hospital networks, disputes over record authenticity, unauthorized modifications, and data tampering are common challenges. Traditional centralized systems are vulnerable to breaches, manipulation, and lack of transparency. This project, **MedChain**, implements a secure patient record management system using blockchain technology, ensuring:

- **Data immutability** via cryptographic hashing and chained blocks.
- **Transparent access** through detailed logging of all operations.
- **Tamper-proof record history**, accessible to both patients and administrators.
- **Efficient consensus** using Delegated Proof-of-Stake (DPoS) for block validation.

Built with Python and standard cryptographic libraries, MedChain is a web-based platform that resolves record disputes by creating a secure, auditable blockchain. Unlike resource-intensive Proof-of-Work systems, it leverages DPoS for efficiency. The project also incorporates a **patient consent workflow**, stake-based delegate voting, **Merkle tree verification**, and comprehensive access logs, ensuring secure, patient-controlled medical record management.

THEORY

1. Blockchain in Healthcare

Blockchain provides: **Immutability**: Records cannot be altered once added, **Transparency**: Patients and auditors can verify histories, **Decentralization**: No single point of control.

2. Delegated Proof-of-Stake (DPoS)

Users **stake tokens**-> Voting power is proportional to stake, **Voting**-> Users elect delegates, **Delegates**-> Authorized block producers, forging blocks in turns, Ensures efficiency compared to PoW.

3. Patient Consent Model

Doctors submit records-> Transactions placed in **pending consent pools**, Patients review-> Approve/Deny transactions, Approved-> Transaction moves to **main pool**-> Ready for forging.

4. Merkle Tree

Each block stores a **Merkle root** of all its transactions, ensuring integrity. Any alteration in transactions invalidates the block.

EXPLANATION

Technologies Used

Backend: Python, Flask, **Frontend**: HTML, CSS, **Cryptography**: RSA keys for signatures, **Consensus**: Delegated Proof-of-Stake, **Data Structures**: Blockchain, Merkle Trees, Access Control Lists

Features Implemented

User registration (Patient, Doctor, Admin) with RSA keys, token-based **staking** and **voting** for delegate election, doctor **record submission** with patient consent workflow, **block forging** by elected delegates, **Merkle root** for block integrity, access logs for auditing, and tamper-proof **patient record history**.

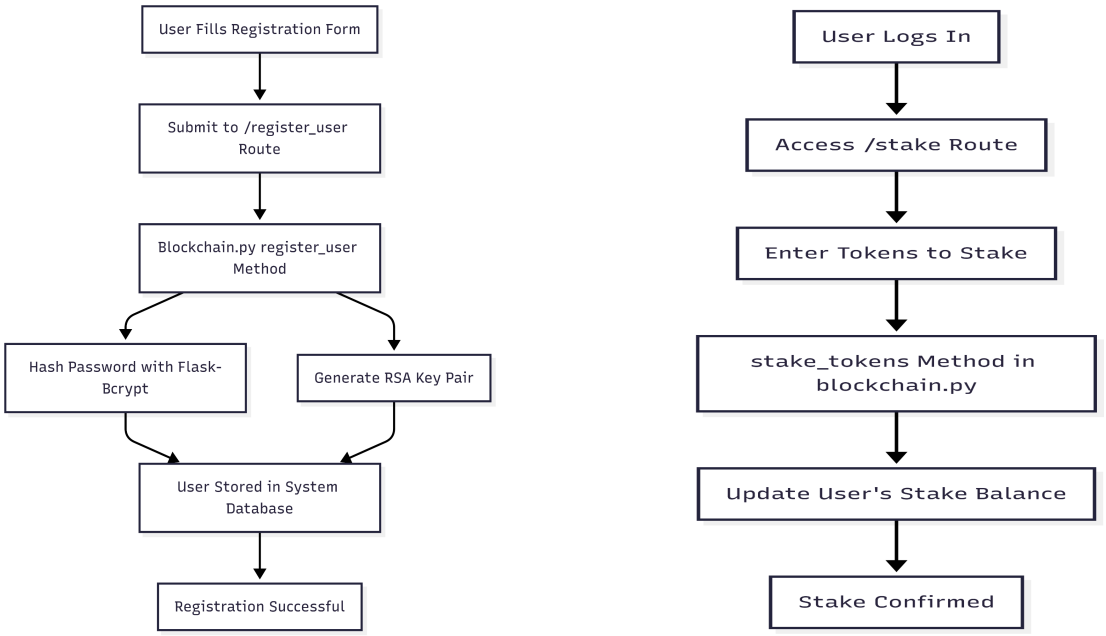


Fig 1.1 (left)**User Registration Flow-** Shows the process of a new user registering in the system. It hashes the password, generates an RSA key pair for secure transactions, stores the user in the database, and confirms registration. (right)**Staking Flow**- Illustrates how a user stakes tokens to gain influence in the DPoS system.

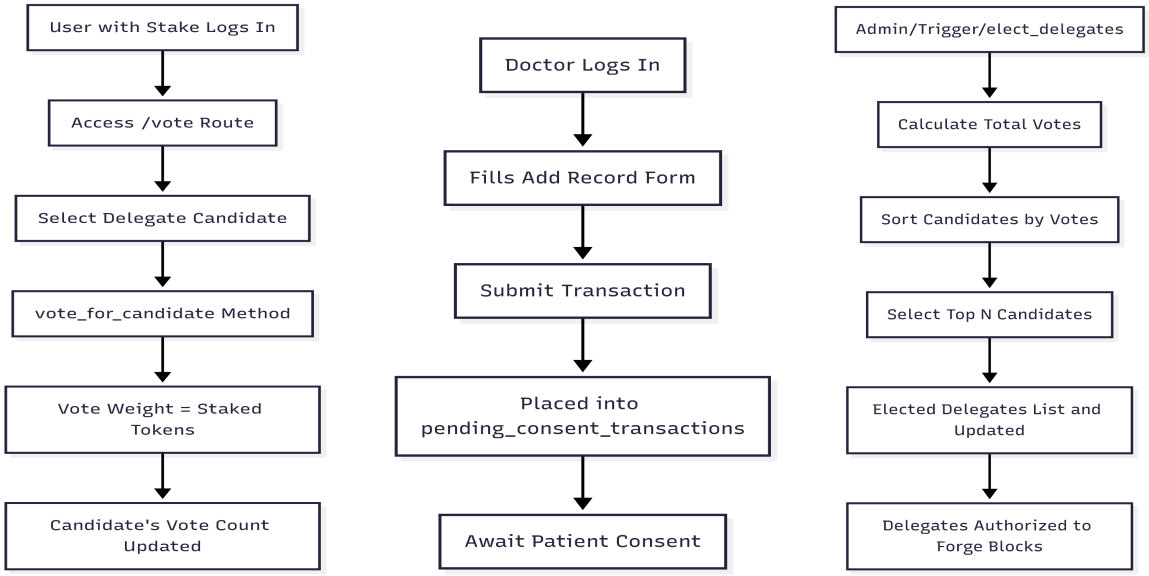


Fig 1.2 (left)**Voting Flow-** Depicts the process where users cast votes for delegate candidates. (middle)**Add Record Flow-** Doctors submit records, initially held in pending consent until patient approval. (right)**Delegate Election Flow-** Shows how top candidates are selected as delegates. Total votes are calculated, candidates are sorted, and the top N are authorized to forge blocks, completing the DPoS election cycle.

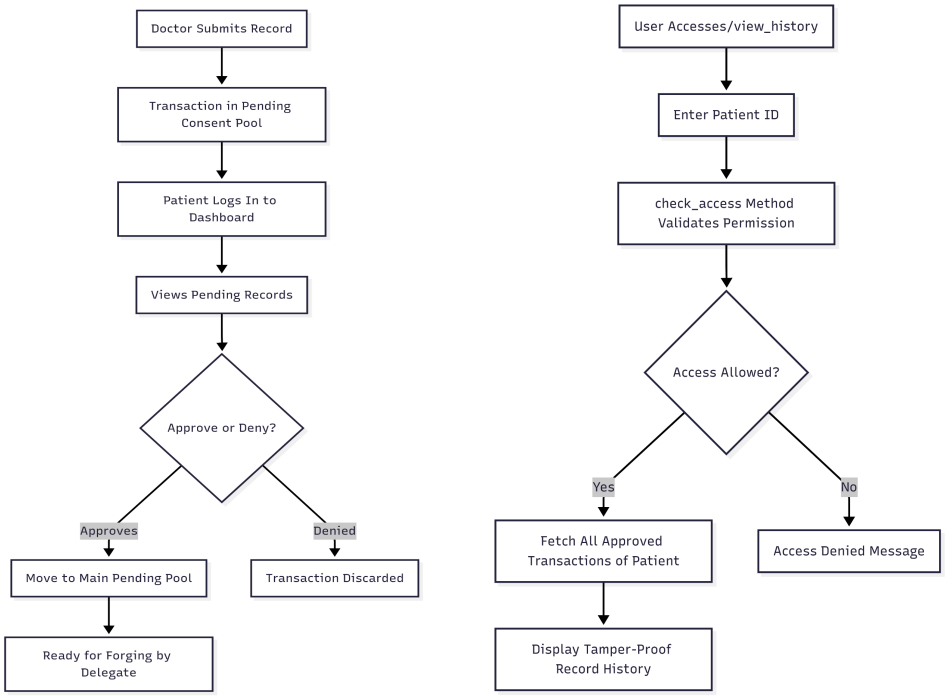


Fig 1.3 (left)**Patient Consent Flow**- Illustrates the two-step patient consent workflow. Approved records move to the main pending pool for forging; denied records are discarded, ensuring patient control over data sharing. (right)**View Record History Flow-** Authorized users view tamper-proof patient records; unauthorized access is denied.

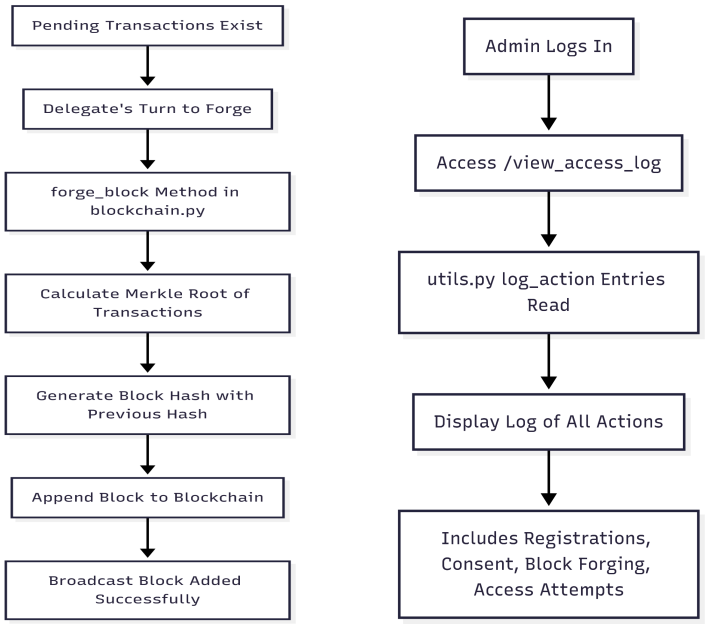
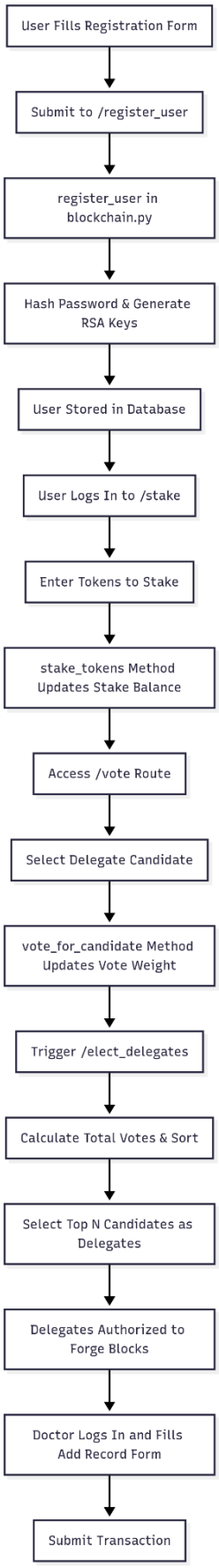


Fig 1.4 (left)**Block Forging Flow-** Delegates forge blocks, compute Merkle root and block hash, and append to blockchain. (right)**View Access Logs Flow-** Admins access a complete log of all actions for auditing purposes.


User Fills Registration Form
Submit to /register_user
register_user in blockchain.py
Hash Password & Generate RSA Keys
User Stored in Database
User Logs In to /stake
Enter Tokens to Stake
stake_tokens Method Updates Stake Balance
Access /vote Route
Select Delegate Candidate
vote_for_candidate Method Updates Vote Weight
Trigger /elect_delegates
Calculate Total Votes & Sort
Select Top N Candidates as Delegates
Delegates Authorized to Forge Blocks
Doctor Logs In and Fills Add Record Form
Submit Transaction

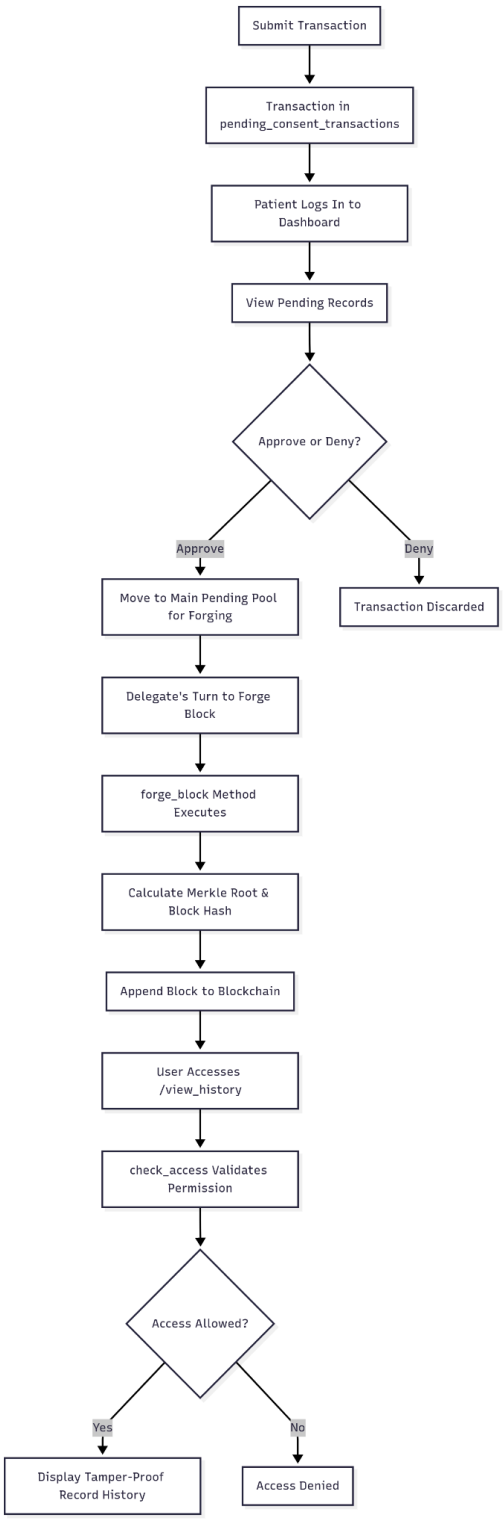


Fig 1.5 This flowchart integrates all operations into a single pipeline, from user registration to staking, voting, delegate election, doctor record submission, patient consent, block forging, viewing history, and accessing logs. It highlights the sequential flow and shows DPoS consensus, patient-controlled approvals, and secure blockchain operations interconnect.

Consensus Algorithm : Delegated Proof Of Stake

Delegated Proof-of-Stake is a consensus algorithm used in blockchains to validate transactions and add new blocks.

- It is a variant of Proof-of-Stake (PoS), designed to be faster and more energy-efficient than Proof-of-Work (PoW).

- Instead of every stakeholder directly validating transactions, DPoS elects a limited number of trusted delegates (also called witnesses) to do the work.

DPOS Implementation in our Project

1. **Staking** : users can stake tokens via '/stake' and 'stake_token' in blockchain.py. The more tokens you stake, the more voting power you have.
2. **Voting** : Token holders vote for a set of delegates using '/vote' route and 'vote_for_candidates' function. Only the delegates with the most votes can produce blocks.
3. **Election** : Top 2 delegates are elected to forge blocks using '/elect_delegates'.
4. **Block Forging** : Only elected delegates can create new blocks using forge_block in blockchain.py.

RESULTS

The project successfully delivers a functional **healthcare blockchain platform** tailored for secure medical record management. By leveraging blockchain technology, it eliminates risks of tampering and unauthorized modifications while ensuring transparency. The integration of **Delegated Proof-of-Stake (DPoS)** consensus provides an efficient and democratic mechanism for block forging, preventing centralization and reducing computational overhead. A robust patient consent workflow guarantees compliance by requiring explicit approval before any medical record is added, strengthening data security and trust. Additionally, comprehensive access logs record all system activities, ensuring accountability and providing administrators with full auditing capability, thereby enhancing the system's reliability and usability.

CONCLUSION

The project showcases how blockchain can transform healthcare record management by integrating **DPoS consensus** with patient-controlled consent. **MedChain** ensures that medical data remains **immutable, and secure**, tackling longstanding challenges of trust and authenticity. By decentralizing authority and empowering patients, it balances transparency with privacy. Future enhancements could include integration with hospital information systems, privacy-preserving techniques like zero-knowledge proofs, and scalability improvements. The system effectively:

- Secures user registration with role-based access
- Records medical transactions with tamper-evident Merkle root hashes
- Employs DPoS for efficient block consensus
- Maintains comprehensive access logs
- Provides tamper-proof patient record history retrieval
