Towards A Block chain Enabled Integrated Library Management System Using Hyperledger Fabric

Zohaib Ahmad Chughtai 1, Sidra chugtai 2, Rizwan Malik 3
[1] Department of Al-Khawarizmi Institute of Computer Science (KICS) University of Engineering and Technology, Lahore, Punjab 54890, Pakistan
[2] Department of Botany University of Gujrat Jalalpur Jattan Road, Gujrat, Punjab 50700, Pakistan
[3] Department of Computer Science University of Gujrat Jalalpur Jattan Road, Gujrat, Punjab 50700, Pakistan
Corresponding Author: Rizwan Malik, Email: rizwanmalik06@gmail.com

ABSTRACT-The Adoption of Integrated Library Management System got an extensive boom in the early 80's. The revolution of cloud computing in Information Technology opens up the gates to many opportunities for system automation but on the other hand, it makes online systems more vulnerable to DoS attacks, viruses, non-authoritative data manipulations and chances of hacking. In the modern technological era data is considered the most valuable resource for a country. Many integrated library management systems perform well to tackle daily base library operations but to cope up with latest threats to library management systems to keep data most secure and transparent, not a single ILMS ensures the secure, fraud less and tamper resistant transaction systems. To solve this problem the author has proposed a model for libraries, which ensure distributed, secure and tamper resistant. All the transactions of library operations are being validated by a pool of nodes and logging into cryptographically encrypted hash-block and each block has the hash value of the previous block thus it makes a chain of blocks which ensures security and transparency of Library Operations. In this paper the author has also demonstrated the implementation of the blockchain based ILMS using Hyperledger Fabric.

Keywords: Blockchain; Hyperledger Fabric; Integrated Library Management System; Cryptography; SHA-256, Security.

1 Introductionon

Libraries are a national asset and the key player to cast a long-lasting impact on the socio-economy of the country. Governments and educational intuitions are now seriously focusing on establishing high-tech libraries for the public mental growth. Academic and Public libraries are considered as free educational resources for the readers. To provide deep and thorough knowledge and better facility to the readers, almost all the libraries have now adopted Integrated Library Management system (ILMS).

In Pakistan, most of the institutes have adopted KOHA as ILMS to manage the daily-based operations of the libraries. Recently the Govt. of Punjab established e-Libraries in 20 districts of Punjab by deploying an open-source library management system. A Union catalogue of Libraries in Punjab has been developed to facilitate sharing of resources across Punjab. Books on the topic of emerging technologies like Artificial Intelligence, Nano Technologies, Material Sciences and related areas are so costly (price ranges from 100 to 3000) that their theft or proxy usage is not bear-able. Some books are rare, even their pirated copies are not available, so it is important to manage its record in such a way that no one can temper it. The modern ILMS are good enough to manage record keeping but failed to tackle security issues like DoS, cyber-attack, viruses, and data tampering and hacking. Tempering in library records results in corruption, which is a big challenge for libraries in the current scenario. Databases of ILMS can be directly tempered, which is a loophole and can only be catered if we adopt blockchain technology to store transactions in a distributed environment. To cope up with the security challenges to ILMS, we have proposed a model for ILMS based on blockchain. All the transactions will be stored in the distributed environment by Hyperledger fabric (a blockchain framework), which is unable to temper. This assures that all the transactions are valid. The target of our system is to achieve transparency in library operations like storing the records of books, issuances, receiving and user authentication etc.

Proposed model is based on the Hyperledger Fabric framework, because this framework is based on a private blockchain network, so no one can enter into the system. Our proposed solution uses this framework due to the following reasons [9]:

1. It is a permissioned network and fits for Library operations because the participants are in an enclosed environment; all the participants belonging to this network have specific identities.
2. The framework is based on modular architecture that is why it is very convenient to adopt in library management.
3. Framework uses channels, which authorises only those users to access the information, who needs to know.
4. Framework runs on the Linux foundation, which is open source and cheap to adopt.

It covers the security challenges discussed above; System is aimed to assure that every transaction of the books will be stored in a distributed environment via blockchain. Through this system, we aimed to provide wallets to the end users integrated with blockchain, through which users can trace back all of its transactions as well as make requests to librarians for new issuance. Currently there is no ILMS which is based on blockchain. This is the first of its kind.

2 Literature Review

Afzal et al. discussed the different challenges that arise for libraries with the evolution of latest technologies in the field of Information Technology [1]. As the information, technology enables library systems to be more efficient, reliable and more networkable but at the same time it makes library systems more vulnerable to DoS attack, viruses, and data tampering and hacking. They discussed comprehensively some of the major issues that to be addressed through information technology itself like: Information Privacy, Information Security and Copyrights.

Machovec et al. discussed the hurdles faced by the llibraries operating standalone and also discussed why Library Networking and Consortia are the need of time [6]. As cloud computing emerged as an efficient solution for many systems which operate standalone for decades ProQuest, OCLC and Ex Libris as one of the primary features of the next generation of ILMS with reference to these features. They also discussed different options to adopt shared LMS which could be citywide, region wide and countrywide. Consortia also identified different challenges regarding adopting the next generation ILS like cost, system selection, scalability and performance, trans-platform integration and among all of these is security as library data hosted on cloud, considered to be secure.

Singh et al. studied two ILMS (Koha 3.2.4 and NewGenLib 3.0) [3]. Authors discussed the capabilities of both ILMS that fulfil the requirement of modern era’s ILMS. For example, price, transparency, community network, system dependency, future version development, system security, usability, granularity, flexibility and user-friendly UIs. But they have not discussed the threats like DoS and single point of failure KOHA and NewGenLib.

All the papers [1] [6] [8] are based on centralised ILMS and discussed its features, although centralised ILMS have ability to secure data and privacy of users but they still could not find detection and avoidance of transaction tempering. For example, super admin of any ILMS could perform manipulations on DB level, which cannot be detected by the system/application. In this regard, blockchain technology is the best solution to make ILMS a tempered resistant system.

Chen et al. described the possible applications of blockchain in different areas but mainly focus in the field of education. They mentioned in their article how the University of Nicosia managed to issue course completion certificates to their students by blockchain technology [3]. Likewise, students at MIT Media Lab would get an assessment-passing certificate whose information is being kept in blockchain. They further explained issues of Fake Degree holder or proxy student enrolment, which can be solved by implementing blockchain solutions in educational institutes. Authors proposed a blockchain model of smart contract powered by Ethereum blockchain network to evaluate a student's learning outcome for a specific course. Their model could be implemented in other applications of education institutes as well like libraries, exams and dues sections.

Nakamoto et al. proposed a new electronic payment method which is based on peer-to-peer communication and named this framework as bitcoin [7]. It is a chain of transaction stored in a block with current hash of the user and cryptographically signed hash of previous user this form a series of linked blocks (blockchain). The purity of blockchain is maintained and impossible to tamper as it contains the hash value of the previous block, which ensures true validation of future transactions. They also gave proof-of-concept of Timestamp Server, Proof-of-work (PoW), Incentive and payment verification techniques to form a framework Bitcoin.

Zyskind et al. paid a serious concern on the level of relay and usage of 3rd party apps in our daily life as it compromises our personal data security by making it extremely vulnerable [10]. They proposed a solution model to overcome the security breaches which accord with the user’s privacy and personal data. User can manage itself so it could minimise the third-party access to the user's data. Author implemented the blockchain framework which enabled blockchain as access-control manager and recorded the data manipulation transactions into blockchain. As the access-control is the major concerned feature in all-online centralised systems, this blockchain model could be implemented in systems like ILMS and other online-centralised systems.

Hoy et al. founded Blockchain technology comparably updated and efficient in order to store online transactions, which are tamper resistant by discussing many applicable fields of blockchain, they emphasised on implementing blockchain in the field of medicine and library [4]. He gave a proof of concept about implementation of bitcoin framework to tackle digital rights Management and access control issues in Libraries of Educational Institutes.

2.1 Research Gap

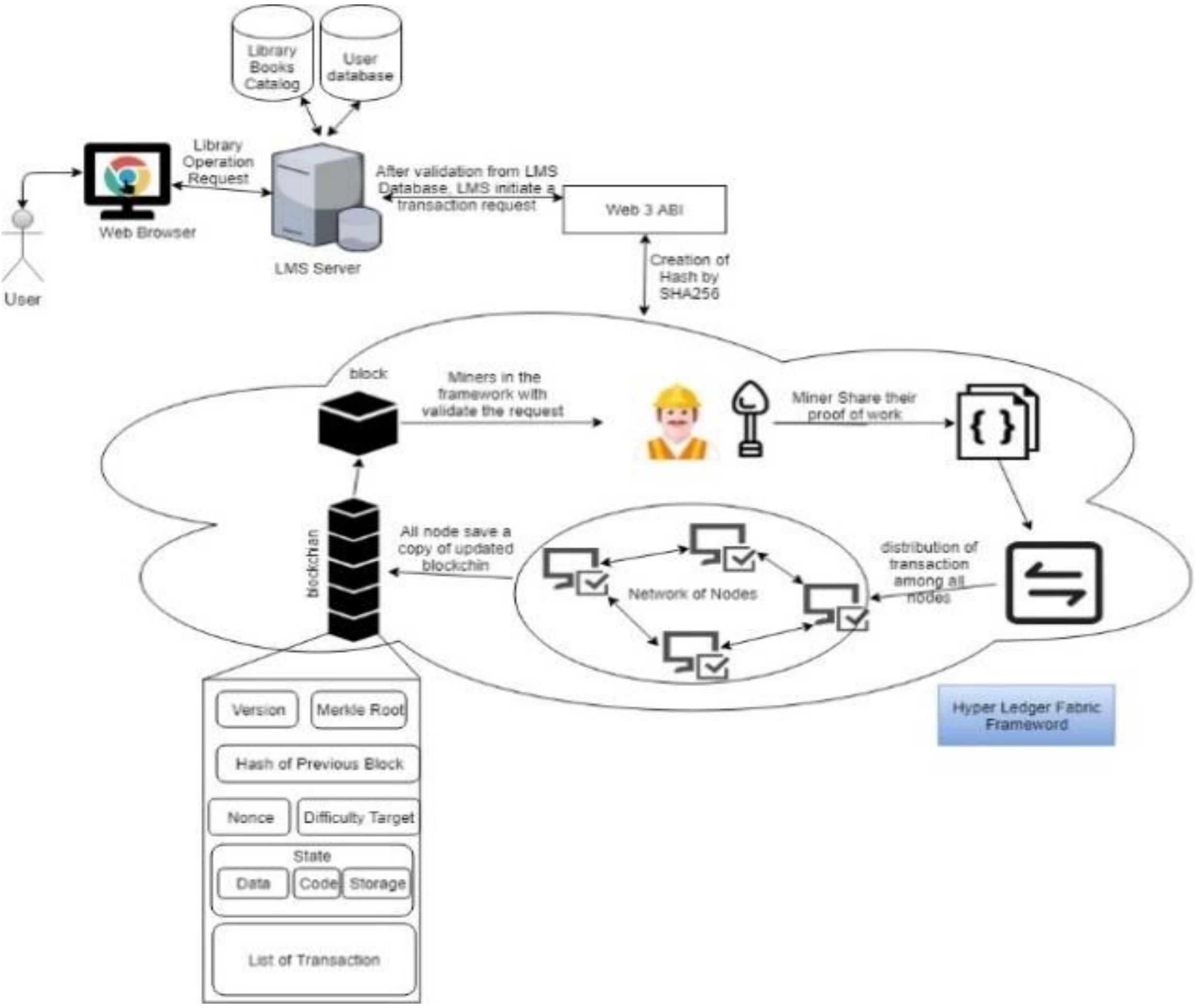
Integrated Library Management System enables its user to perform daily based library transactions in a more efficient way but there are many security concerns that arise when a system goes online. Many security algorithms are there to ensure the security of the system but failed to detect and avoid the tempering of ILMS transactions in Database. Specifically, tracing direct manipulation in the database is difficult. This loophole can be catered by blockchain technology, which makes an ILMS system a tamper-resistant system.

2.2 Scope of Work

This proposed model for ILMS via permissioned Blockchain will help any library to ensure the security of the records of important, rare and costly books against manipulation or losing data and no one from the outside can enter into this system without permission. This model has three subsystems: the first is for user authentication, the second provides the facility to manage the catalogues of books, and the third is for transactions of the books which keeps record of all the transactions carried out in the whole system.

3 Proposed Model for Library

Our proposed model for the LMS is based on Hyperledger Fabric and it has three modules as shown in Fig. 1.


Library Books Catalog
User database
Library Operation Request
Web Browser
User
LMS Server
After validation from LMS Database, LMS initiate a transaction request
Web 3 ABI
Creation of Hash by SHA256
block
Miners in the framework with validate the request
Miner Share their proof of work
{ }
blockchain
All node save a copy of updated blockchin
Network of Nodes
distribution of transaction among all nodes
Hyper Ledger Fabric Frameword
Version
Merkle Root
Hash of Previous Block
Nonce
Difficulty Target
State
Data
Code
Storage
List of Transaction

User Authentication Module

User Authentication Module to verify the registered users, an interface provided to the end users with the help of an API on backend, users authenticated before they login, and so only authenticated users can use LMS. It has two main roles: students as well as librarian, students have limited access and they can only search books while the authorised librarian has full access to perform transactions.

1. **Catalog Management Module**

Catalog management module enables users to search the books through a web-based interface.

Figure 1: System Design of Proposed Model

Catalogue is the collection of books containing all the metadata of the books like author name, title, edition, cost, year of publication, ISBN number with the availability of the book.

2. **Transactions Management Module**

The transaction management module covers all the basic operations of the library like issuance and receiving of the books by involving Hyperledger fabric as shown in Fig. 2, this will ensure the validity of the transactions, the detail steps of transaction is given as:

- Any node from the network submits a request to the endorsement peer through the chain code.

- Endorsement peer replicates it and stores one copy in the local storage by using gossip protocol, it also distributes this copy to other peers.
- The endorsement peer sends back the data to the node that has generated the request.
- After approving, the first node sends a proposal to the sorting service node and the output of the sorting service spreads to the channel. Then all peers verify the transaction by using a hash of the data.
- After submission of a block, the authorised peer inspects that either the received data endorsed by chain code or not. If yes, then it will store the received data into the ledger, synchronise all the peers, remove all data from temporary storage and update the state of the related data in the repository.

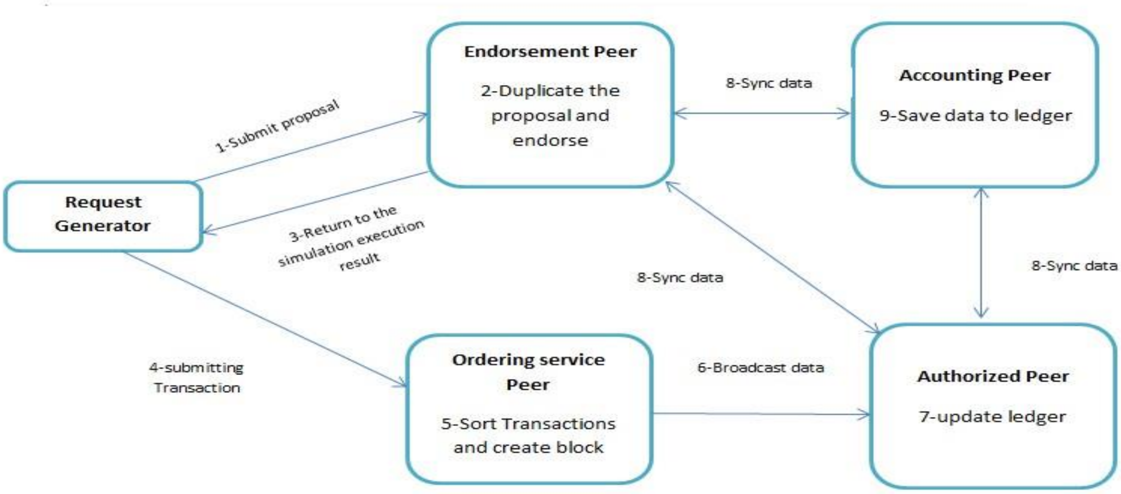


Figure 2: Transaction Flow Diagram

3.1 Core Technologies for a Blockchain

Several functions are involved in blockchain technology depending upon their needs. To make transactions more secure different hashing algorithms can be used to create the hash of the transaction. The motive to include this function is to map the information or data into fixed size of length although the data length is not fixed. A hash function gives a unique connection between the input data or information and the value of the hash, and short-term representation of a long data. For our proposed model SHA-256 [2] hash algorithm is used. The SHA-256 is a successive hash function (called as SHA-2 overall), and the strongest amongst all the available functions. Although the SHA-256 is not much more complicated than the SHA-1, it is still not compromised in some way. It makes a good partner for 256-bit key AES. It is defined in the 'FIPS 180-4' standard in NIST. Provide several test vectors to apply for the verification.

Keeping the transaction's Timestamp in this system is extremely important. It is used to produce the evidence of sequential order of the transactions and for the block's creation time. In the context of the Library Management System, the system will be able to produce results that will determine the authentic time record for all transactions and to avoid data tampering. Nodes generally count noodle colleagues based on timestamps, which are sent to the version message as a node connection.

1. SHA-256 HASH ALGORITHM: It is a cryptographic hash function. Hash value h is created by a capacity H of the structure h = H (I), where I is an input and H (I) is fixed-length hash value which is produced by the hash function. In a cryptographic hash algorithm, H (I) is padded and divided into small chunks and sent to a compression function consecutively, which gives a fixed-length hash value. In hash function, message digest is the value of individual blocks, which is used by the compression function to find the final value of that information [2].

2. TIME STAMP: Timestamp is a unique identifier, which creates transactions in ascending order [5]. There are few transactions like T1, T2, T3, T4 and timestamp assigned are (10, 20, 30, 40) respectively, T1 is the oldest transaction because it was created before the occurrence of T4 and T4 is the youngest transactions and

   TS(T1) < TS(T2) < TS(T3) < TS(T4)

   Read timestamp is the highest transaction timestamp value that has performed read operation successfully. Write timestamp is the highest transaction timestamp value that has performed write operation successfully. Basic timestamp ordering protocol this timestamp ordering protocol says that:

   ```
   If (read-Ts(x)>Ts(Ti) or write-Ts(x)>Ts(Ti))
   {abort Ti and rollback; }
   else {write(x); write-Ts(x) = Ts (Ti);}
   Transaction Ti issues a read(x) operation
   if (Read Transaction(x) > Transaction (Ti) OR Write T
   {abort Transaction and rollback;
   } else {
   Transaction Issues the write operation
   }
   Transaction Ti issues a Write (x) operation
   ```

3.2 Summarized Process for System

The proposed model has three types of processes. These have different scenarios depending upon the situation. First, specific authorised persons can add books in the book catalogue along with specific required information. Sudo-code for adding a book in the catalogue:

```
Function Add Book (Arguments) {
// TODO Only Specific member will be able to add books Encrypt ISBN using sha-256
Set value for the new added book along with encrypted ISBN, author name, timestamp etc. in book store
Set the address of book inside book store
Send message
End
}
```

Figure 3: Sudo-Code for Adding a Book In The Catalogue.

In the case of students, users can login and search for books. If the student wants to issue a book, he/she requests the authorised person (librarian) along with that book. The Librarian in our case is considered an authorised node that scans the ISBN of the book and sends the request to the blockchain network along with student private data. All nodes of blockchain verify the request and check the student's transaction history of the book, if the request is valid then the book is issued to the student by adding timestamp using timestamp generation algorithm and generating hash code using SHA-256 algorithm. This transaction is saved and distributed among all the nodes as shown in Fig 4.

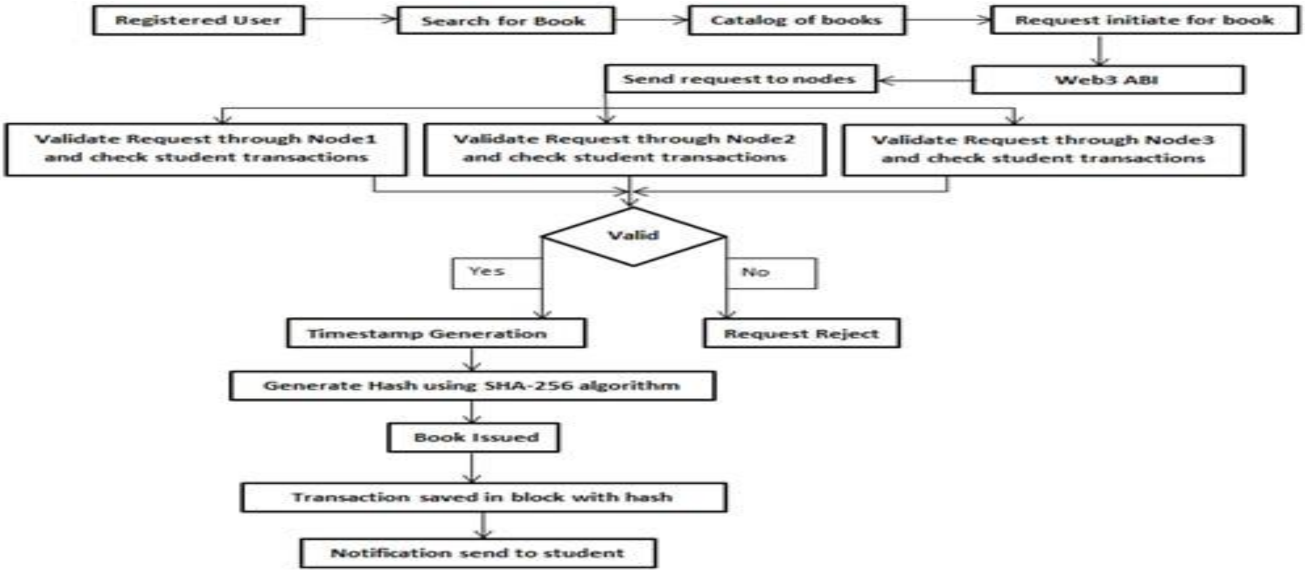

Registered User
Search for Book
Catalog of books
Request initiate for book
Web3 ABI
Send request to nodes
Validate Request through Node1 and check student transactions
Validate Request through Node2 and check student transactions
Validate Request through Node3 and check student transactions
Valid
Yes
No
Timestamp Generation
Request Reject
Generate Hash using SHA-256 algorithm
Book Issued
Transaction saved in block with hash
Notification send to student

Figure 4: Process Flow for Book Issuance

```
Function Get Book (Arguments) {
First check ether borrower is valid for it
If yes then
        Check ether book is available
         If yes then
                Issue book along with borrower id, information
                Of book, date of issue and date for return
         End
    }
```

Figure 5: Sudo-Code for Book Issuance

In case if student come to return the book, the registered node after receiving the book, initiates request for book returning by scanning the barcode of particular book, the request sent to all the nodes, these nodes verify the request, after verification state of the current book updates as shown in Fig 6.

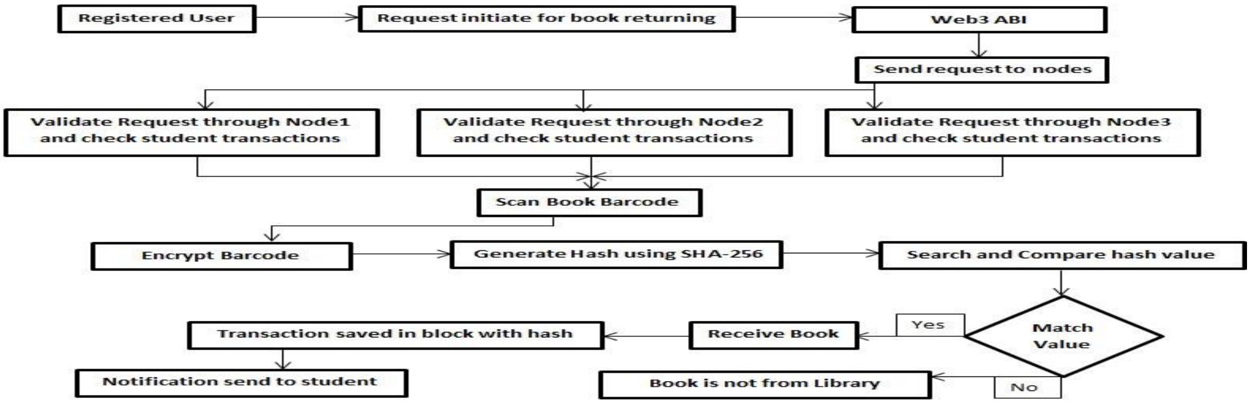

Registered User
Request initiate for book returning
Web3 ABI
Send request to nodes
Validate Request through Node1 and check student transactions
Validate Request through Node2 and check student transactions
Validate Request through Node3 and check student transactions
Scan Book Barcode
Encrypt Barcode
Generate Hash using SHA-256
Search and Compare hash value
Match Value
Yes
No
Receive Book
Transaction saved in block with hash
Notification send to student
Book is not from Library

Figure 6: Process Flow for Book Receiving

```
Function Return Book (Arguments) {
Open borrower data using id
Calculate fine by comparing return date specified at
the time of issue and the current date
Update borrower account by enter returning information
Update record of the returned book
End
}
```

Figure 7: Sudo-Code for Book Receiving

4 Conclusion

The modern ILMS are good to serve the operations of Library, but could not assure security threats like DoS attack, viruses, data tampering and hacking etc. To cater the latest security challenges to ILMS we have proposed a model for a LMS based on blockchain. All the transactions will be stored in the distributed environment by blockchain Hyperledger Fabric, which is unable to modify or temper. This assures the guarantee that all the transactions are valid. The target of our system is to achieve transparency in library operations like issuance and receiving and user authentication etc. Currently there is no ILMS which is based on blockchain. This is the first of its kind.

References

1. A.-S. W. Afzal, M. Nasser et al. (2001). “Digital age: Challenges for libraries,” Information, society and justice journal, 1(1), 43–48.
2. Ahmad and A. S. Das. (2005). “Hardware implementation analysis of sha-256 and sha-512 algorithms on fpgas,” Computers & Electrical Engineering, 31(6), 345–360.
3. G. Chen, B. Xu, M. Lu, and N.-S. Chen. (2018). “Exploring blockchain technology and its potential applications for education,” Smart Learning Environments, 5(1), 1.
4. M. B. Hoy. (2017). “An introduction to the blockchain and its implications for libraries and medicine,” Medical reference services quarterly, 36(3), 273–279
5. W.-T. K. Lin and J. Nolte. (1983). “Basic timestamp, multiple version timestamp, and two-phase locking.” in VLDB, 83, 109–119.
6. G. Machovec. (2014). “Consortia and next generation integrated library systems,” Journal of Library Administration, 54(5), 435–443.
7. S. Nakamoto et al. (2008). “Bitcoin: A peer-to-peer electronic cash system,”
8. M. Singh and G. Sanaman. (2012). “Open-source integrated library management systems: comparative analysis of koha and newgenlib,” The Electronic Library, 30(6), 809–832.
9. M. Valenta and P. Sandner. (2017). “Comparison of ethereum, hyperledger fabric and corda,” [ebook] Frankfurt School, Blockchain Center.
10. G. Zyskind, O. Nathan et al. (2015). “Decentralising privacy: Using blockchain to protect personal data,” IEEE Security and Privacy Workshops. pp. 180–184.