Implementation of Blockchain Technology in AndhraPradesh Medical Council (APMC) for Certificate Verification

[1]Erina Kiran Kumar , Scientist-D, NIC [2]S .Madhusudhana Rao, Scientist-F, NIC,
[3]Vinay Sowpati, Scientist-C, NIC [4]Dr PVSS Gangadhar , Scientist-E, NIC.

ABSTRACT: In an increasingly interconnected world and with the constantly increasing and Technological advances in the last decade, it is foreseen many cyber threats in this digital world. It is necessary to replace or develop other technologies to preserve digital systems from many security threats and adds layers of protection and trust. A powerful opportunity can emerge from utilizing Blockchain Technology. This technology is expected to develop various industries objectives such as economic, society, medical, businesses, and education. This paper explains the functioning of "Blockchain Technology" and critically assesses its potential role in improving services in issuing the registration certificates. The paper concludes that a Blockchain is a peculiar engineering design whose only advantage is in removing third party intermediation to allow for the creation of digital certificate, and is unlikely to offer economic advantages for any commercial problem other than the one it was specifically engineered to solve.

Index Terms: Blockchain in APMC, Hyperledger, Smart Contract, Verification &Validation

1. Introduction

Blockchain as an emerging technology is poised to revolutionise how we perform transactions digitally. This distributed ledger technology allows storage of information securely across multiple systems to enable peer-to-peer transactions in a trustworthy manner. There are huge data sets in government which are being used and updated by various agencies. Ensuring consistency of data and tracking the modifications is a challenge especially when the data is highly volatile.

Blockchain technology would provide solution for maintaining such huge data sets and help in insuring consistency. Based on Blockcerts, a series of cryptographic solutions are proposed to resolve the issues above, including, utilizing a multi-signature scheme to ameliorate the authentication of certificates; exerting a safe revocation mechanism to improve the reliability of certificates revocation, establishing a secure federated identification to confirm the identity of the issuing department and summarize a set of future research directions based on the challenges and gaps identified in existing research work. Our Research study aims to highlight the importance of BlockChain-App V&V (Verification and Validation) and pave the way for a disciplined, testable, and verifiable BlockChain development.

1.1 Present System Process Flow:

APMC is issuing various services to these medical candidates like those who wanted do the medical practicing , who seeking further higher degrees / Additional Qualifications or the candidate who wanted to do practicing in other states need to take certificate from APMC. Andhra Pradesh Medical Council (APMC) is the nodal agency for providing various services to the Doctors which are listed below.

1. Provisional Medical Registration
2. Final Medical Registration
3. No Objection Certificate (NOC)
4. Renewal of registration
5. Re-Registration
6. Duplicate Registration
7. Good Standing
8. Additional Qualification
9. Continuous Medical Education (CME)

Generally, in India, the Medical Students study for 4.5 years of course in Medical College and after completion of the course, he/she needs to apply to the APMC for the Provisional Registration which is mandate to do the internship in any medical college hospital. After completion of the internship, the student has to apply for final medical registration for the permission to do the medical practice or for any services like PG studies, jobs etc. And this registration certificate is valid for 5 years only. After that he/she needs to do renewal of the certificate. If he/she completes the PG studies, he/she needs to get registered the additional qualification at APMC. If the doctor wants to settle down in another state, then he/she has to get the NOC from APMC and get the final registration from that state Medical council. The doctor can also get the duplicate registration if he/she loses the final registration certificate. The doctor needs to get some credit points yearly by attending some seminars and conferences which will be useful for getting the Good Standing certificate.

1.2 Challenges

The Doctor who is seeking various services from APMC, needs to apply across the counter by paying the necessary fees against the required service . Later it goes for necessary series of approvals. Finally it gets approved by APMC authorities and will issue the necessary services certificate to the candidate. As the Government who spend heavily on the verification of these documents. Since the volumes are large, a small fraction of fake documents entering the system is alarming and a great cause for concern as this could lead to ineligible candidates gaining benefit while depriving the deserving candidates. A lot of effort and time of student is spending in obtaining these certificates. Multiple visits are required at times to obtain such educational documents. A few of such

documents even have a validity period thereby making it is a periodic task for a student. On the other hand is equally difficult for the validating these documents.

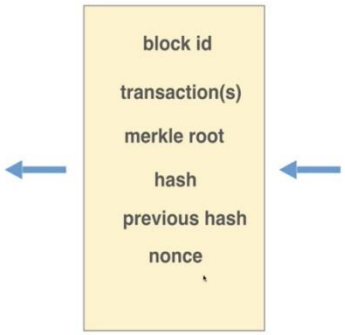
2. Overview of Blockchain Technology

Blockchain Technology would provide the necessary impetus to move form demand-based process of service delivery to an eligibility-based system. Immutability of data in the Blockchain and the transparency it provides would make it possible to provide the necessary trust required to automatically initiate service delivery by executing the smart contracts stored in the Blockchain through a consensus process. The emergence of Blockchain Technology holds promise for the government to faster trust and greater transparency in service delivery. This technology promises to provide tamper-proof storage of key transactions thereby eliminating intermediaries of trust. In addition to understanding the technology, determination of the right applications of the technology is a critical factor to accelerate its adoption. It is a form of storing information that prevents anyone from changing, hacking, or cheating it.

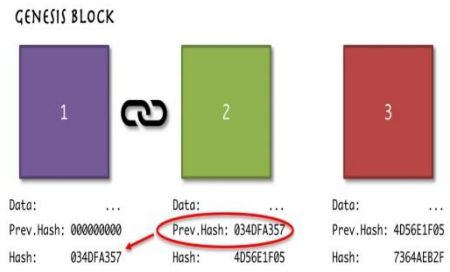
Every transaction in this ledger is authorized by the digital signature of the owner, which authenticates the transaction and safeguards it from tampering. Hence, the information the digital ledger contains is highly secure**.** Blockchain Technology can be defined as a time-stamped and tamper-resistant distributed digital ledger. It can allow validate and secure the transactions and update records in a transparent, synchronized, and decentralized with the consensus of a majority scheme and is considered a part of the fourth industrial revolution.

2.1 What is Block ?

Block: A block is the one which contains transaction data and ready to join the network. A block contains information like block id, current hash, previous block hash, message, date etc depending upon the type of application. The initial block in a Blockchain is known as Genesis block where the previous hash value of this block will be 0 since it doesn`t have any previous blocks. The hash value of this block will be previous hash value of the next block and it continues.



Blockchain Node



Blockchain Network

2.2 Key elements of Blockchain

Distributed ledger technology

All network participants have access to the distributed ledger and its immutable record of transactions. With this shared ledger, transactions are recorded only once, eliminating the duplication of effort that's typical of traditional business networks.

Immutable records

No participant can change or tamper with a transaction after it's been recorded to the shared ledger. If a transaction record includes an error, a new transaction must be added to reverse the error, and both transactions are then visible.

Smart contracts

To speed transactions, a set of rules — called a smart contract — is stored on the Blockchain and executed automatically. A smart contract can define conditions for corporate bond transfers, include terms for travel insurance to be paid and much more.

2.3 Why is it so revolutionary?

The technology can work for almost every type of transaction involving value, including money, goods, certificate verification and property etc. Its potential uses are almost limitless. Blockchain could also help to reduce fraud because every transaction would be recorded and distributed on a public ledger for anyone to see.

Blockchain a data or a node is validated only when multiple parties approve it. So, the system would be Reliable and Authenticated at any instance of time.

Now, the issue of tampering is solved. The next issue that comes into the picture is time consumption for validation. The system that we will be building will not only validate the certificates but also generate certificates. So it is like killing two birds with one stone. As everything is automated, it takes mere seconds to validate the document.

Since everything will be stored digitally, a student doesn't need to worry about losing or damaging the certificate in the process of validation. This proposed system not only removes the loopholes in our current system but also gives us an effective and concrete solution.

3. BLOCKCHAIN-BASED PROPOSED CERTIFICATE STORAGE

By using technical collaboration with Centre of Excellence for Block Chain Technology of National Informatics Centre [NIC] under Ministry of Electronics and Information Technology (MeitY), Govt. of India, it is proposed to build a solution using Blockchain Technology named as "Registration {Blockchain} Certificate Documents [RBCD] ". The APMC will send meta data of the services rendered to the Doctors. Blockchain Technology ensures that Medical Registration documents are recorded in a secure and tamper proof manner. These documents can be accessed online in a trusted and verifiable manner. Various services Certificates issued by the APMC have been established using Block Chain Technology to record the certificates in a linked chain

structure. The result certificates are kept in a distributed manner at different locations involving multiple stakeholders protecting it against any attempt of tampering.

This [RBCD] network is established with nodes at different locations of NIC. Presently, the [RBCD] is managed by NIC at its data centers. One of the challenges faced is the verification of the authenticity of certificates produced by the doctors for additional qualifications, NOC, Renewals, Good Standing etc. The verification of correctness and genuineness of the medical registration certificate with the concerned universities or boards requires considerable effort and processing time. Hence most of the times, the institutes/organizations insist on production of the original certificate by the doctors. Various services [RBCD] Documents addresses these challenges regarding verification of documents produced by doctors. Blockchain Technology enables the data in a distributed ledger with ownership of all participating stakeholders. The data is recorded in the chain based on the consensus among the stakeholders and simultaneously replicated at all the locations in the distributed network of Blockchain nodes. This eliminates the dependency on a third party for verification. Data is linked and stored with cryptographic security so that it is immutable and traceable. The linking of the blocks in the block chain ensures that they cannot be tampered with and the data is trustable as it can be verified across the participating stakeholders. A process for any change in the certificate details can implemented in the APMC applications that would initiate a transaction to the Blockchain system.

3.1 **Proposed Work Flow** Diagram

The proposed work flow of [RBCD] validation within the APMC and other stakeholders. Initially, the doctors applies for the Final Medical Registration and gets the digital registration certificate. That Blockchain technology is applied on this certificate with necessary encryption and alogorithms. That will be stored in all nodes of [RBCD] network. If the doctor goes to any interview at Govternment or private organization or registers in another Medical Council across the states of India or outside India too, the certificate validation will be easier by checking the genuineness of the certificate by checking it in [RBCD] web portal.

Workflow diagram of the [RBCD]

4. APPLICATION STRUCTURE AND FUNCTIONALITIES

4.1 Tools and Platforms:

To develop application Embark framework (v 4.0.0) [20]has been chosen , Embark is a fast, easy to use, and powerful developer environment to build and deploy decentralized applications, also known as "DApps". It integrates with **Ethereum** blockchains, decentralized storages like **IPFS** and **Swarm**, and decentralized communication platforms like **Whisper**. For the Storage part, blockchain part, Front-end part and Back-end part of the application offers complete environment configuration. Solidity is a language used for creating smart contracts which is then compiled to a byte code which in turn is deployed on the Ethereum network. (v0.8.x) [20].

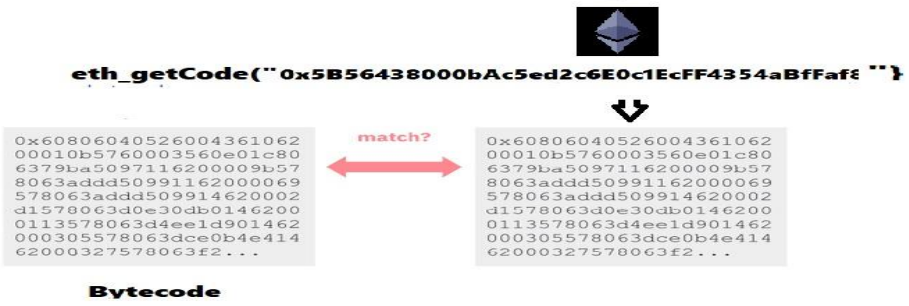


Fig. Verification.

Steps in Verifying a smart contract:

a) Input the source files and compilation settings to a compiler.
b) Compiler outputs the bytecode of the contract.
c) Get the bytecode of the deployed contract at a given address.
d) Compare the deployed bytecode with the recompiled bytecode. If the codes match, the contract gets verified with the given source code and compilation settings.
e) Additionally, if the metadata hashes at the end of the bytecode match, it will be a full match.

Verification Tools:

Sourcify is a tool for verifying contracts that is open-sourced and decentralized. It only verifies contracts on different EVM based networks. It acts as a public infrastructure for other tools to build on top of it, and aims to enable more human-friendly contract interactions using the ABI and NatSpec comments found in the metadata file. Sourcify supports full matches with the metadata hash. The verified contracts are served in its public repository on HTTP and Internet Planetary File System (IPFS), which is a decentralized, content-addressed storage. This allows fetching the metadata file of a contract over IPFS since the appended metadata

hash is an IPFS hash. Additionally A contract can be verified by providing the metadata file and source files over its API. This property complemented with the immutability of the Ethereum Blockchain records creates a tamper-proof system.

To access and utilize the Ethereum network a wallet is a needed by the user. And also web browser such a Google Chrome or Mozilla Firefox should be installed and enabled Metamask extension [23]. MetaMask is a browser plugin that serves as an Ethereum wallet, and is installed like any other browser plugin. Once it's installed, it allows users to store Ether and other ERC-20 tokens, enabling them to transact with any Ethereum address.By connecting to MetaMask to Ethereum-based dapps, users can spend their coins on trade in a decentralized exchanges (DEXs). And also users have the balance information, address credentials and functionalities for interaction with application located in the Ethereum Blockchain.

Integration of IPFS with Blockchain:

It is possible to address large amounts of data with IPFS and to place the immutable, permanent IPFS links into a blockchain transaction.

As this RBCD application uses the Blockchain Infura development suite that provides instant and scalable Application Programming Interface (API) access to the Ethereum network and the Internet Planetary File System (IPFS) [23]. With the Infura service, the application attaches to the Ethereum network without the use of a fully functional Ethereum node. This gateway service for easier deployment of distributed applications (DApps). Infura development suite offers a nice gateway to the IPFS[23] storage, to access the application data. IPFS[23] is protocol for peer-to-peer storage and sharing of files in a distributed fashion. The application content is recorded and hosted on the IPFS network, except for the IPFS[23] record addresses, which are kept on the Ethereum Blockchain. The content on the IPFS storage cannot be erased or modified with the current version of IPFS[23] protocol.

4.2 [RBCD] Design Methodology

The application consists of two functional parts: one part is the certificate identification (CID) number storage procedure on the Ethereum Blockchain via Smart contract and the other segment is the front-end and the back-end of the application stored on the IPFS network.

There are two ways to verify the Medical Registration documents:

(i) By accessing the portal and entering the basic details of the Doctor like Final registration number etc. for viewing the registration documents.

(ii) The institutes can register with the APMC and use the bulk verification tool and API based verification modes.

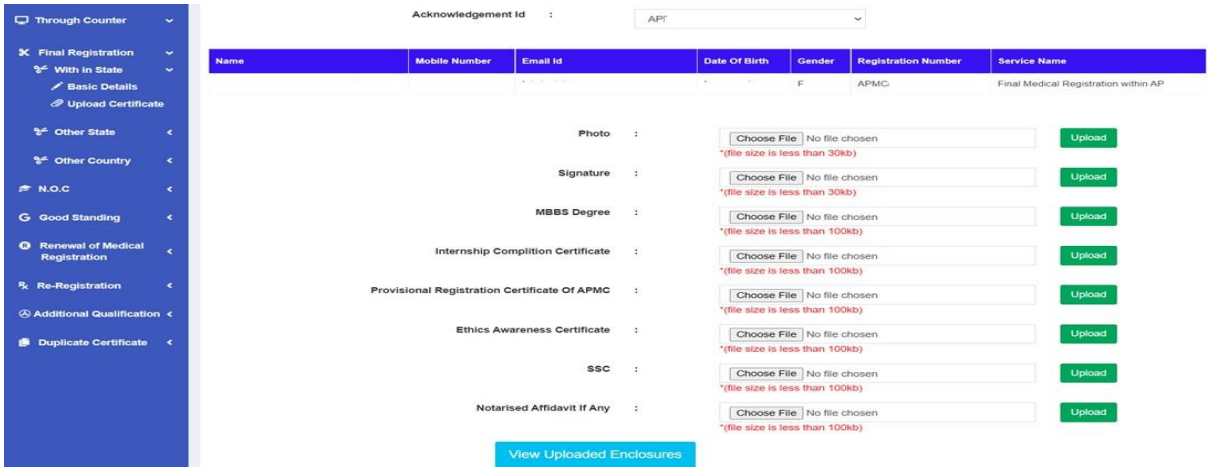


Figure Application Screen

II. Users of Registration {BlockChain} Documents

Registration {BlockChain} Documents [RBCD] provides the mechanism for the educational institutes, companies and other stakeholders to verify online the details of the Registration Certificate genuineness of the Doctors, who apply for the PG Qualifications (MS/MD) education or job. It also helps in counselling and registration process, by integrating the systems with plug-in interfaces.

Main users of this chain are;

- Doctors
- Medical Colleges
- Hospitals
- Government Organisations
- Private Industries

There are different roles in APMC in finalizing and issueing the Registration Certificate. They are

1. Registration Counter
2. Cash Counter
3. Administration Counter
4. Assistant Registrar Counter
5. Registrar Counter
6. Dispatch Counter

The doctor approaches the Registration counter and submits all relevant documents required for the services he/she opts for. If the doctor details are correct and then they will be given a declaration form to sign on that document. Once the doctor submits the

signed declaration form, he/she has to pay the necessary amount for those services opted at the Cash Counter in digital mode (Debit Card/Credit Card/Phone Pay/Google Pay etc). The doctor has to submit the documents to the Admin Counter for the scanning of the documents of the doctors. After the approval of the Admin Counter, the Assistant Registrar will generate the QR code of the certificate. After the approval of Assistant Registrar, the Registrar approves the certificate to generate e-Certificate with digital signature of the Registrar. Blockchain Technology will be applied to the e-certificate generated by the Registrar and it will be stored in all nodes of [RBCD] network to sustain more authenticity and security of the document. Presently, APMC's registration documents of the calendar year 2022 are going to store in the Blockchain and gradually APMC would append registration documents for the previous years.

4.3 Benefits

This Registration certification system shall facilitate the Doctor, Medical Colleges, Government and Non-Government agencies to access and share tamperproof record of Registration certificate details. The system will reduce the errors in manual verification of the document. The process of preparing the eligibility list would be simplified and automated due to the availability of all necessary data brought a resilient, tamper-proof system.

4.4 Features of the solution :

a) The blockchain enabled system created immutable records for APMC for various services rendered to the candidates, which are then digitized and stored permanently on the system, with the ability to track any change in meta data of these certificates issued to the candidates. Any new transaction (such as further change of mistake in Name, Father Name or date of birth, qualification, medical college, pass year, course name etc) gets recorded on the blockchain immutably while remaining available to other stakeholders .

b) Facilitating the Doctor, Medical Colleges, Government and Non-Government agencies to have access to tamperproof record of registration certificate details. This system will reduce the errors in manual verification of the document. The process of preparing the eligibility list would be simplified and automated due to the availability of all necessary data from a single source. The establishment of the registration certificate chain will change the way the Government processes applications for admission, recruitment, medical practice and various other government initiatives. This system could pave the way for entitlement based service delivery.

c) The banks and financial institutions can also use this system for sanctioning of educational loans and merit-based scholarship based on the qualifications of the applicants. One can verify the authenticity of the certificates even after several years of issuance. It will provide the trail of all the insertions or changes made on a particular certificate.

d) Blockchain ensures that docotors cannot alter their grades, degrees, and certification, thus offering employers the guarantee that the job applicants indeed have the necessary skills to succeed in the workplace. Thus, blockchain becomes a "trust anchor of one truth for credentials". Additionally this anchor also offers the opportunity to create better matches between job seekers and employers. More broadly, as distributed ledger technologies support learning and secure registration records, they enhance the relationships among "Medical colleges, universities, Hospitals and their contributions to society" through the integration of trust and transparency in the skills transactions and sharing processes.

e) Blockchain is a powerful technology to issue, establish and preserve a cryptographically secure, shared, and distributed ledger for transactions. Digital certificates powered by blockchain don't need intermediaries to send or verify. Hence, it improves efficiency, secures identity, and ensures tamper-proof data.

f) Since there would be no central point of failure given blockchain's decentralized nature. Hence, you are better in a position to withstand malicious attacks. If anybody modifies or tampers with any certificate, there will be evidence of tampering for everyone to see. The decentralized nature of blockchain denotes that it's almost impossible for anyone to modify or falsify the records.

g) With Blockchain technology, it is as simple as clicking on a button to have all of your digital certificates issued and credentials secured on the Blockchain.

5 CONCLUSION :

The development of distributed and secure electronic systems has become an important subject in line with the development of the digital world. The application of Blockchain technology is an excellent example of these systems that provides exciting features such as transparency, trust, and decentralization with untampared and permanents data records. It is crucial to enhance and simplify the administrative procedures. The current registration certification procedures are prone to falsification, and are very time consuming and expensive for the Doctors. The use of the blockchain technology will have immense impact on the registration certification processes by decreasing the bureaucratic procedures, shorten the time for registration certificate verification and skip the third-parties in the processes. This application is proof for the feasibility of the blockchain technology and the registration certification procedures, by offering transparent, reliable and robust mechanism to prevent the malicious activities in health industry.

6:References:

1. Sayed, R. H. (2019). Potential of blockchain technology to solve fake diploma problem. University of Jyväskylä, JYX Digital Repository.
2. Buterin, V. et al. (2014). Ethereum white paper: A next- generation smart contract and decentralized application platform. http://blockchainlab.com/pdf/Ethereum_white_paper-_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf, 2014.
3. Oliver, M., Moreno, J., Prieto, G., & Benitez, D. (2018). Using blockchain as a tool for tracking and verification of official degrees: business model.
4. Tariq, A., Haq, H. B., & Ali, S. T. (2019). Cerberus: A blockchain-Based Accreditation and Degree Verification System. arXiv preprint arXiv:1912.06812.
5. Wegelid, F. (2019). Storing digital certificates using blockchain. Lund University.

6. Olson, K., Bowman, M., Mitchell, J., Amundson, S., Middleton, D., & Montgomery, C. (2018). Sawtooth: An Introduction. The Linux Foundation.
7. Shah, M. & Kumar, P. (2019). Tamper proof birth certificate using blockchain technology. Int. J. Recent Technol. Eng. (IJRTE), 7.
8. Baldi, M., Chiaraluce, F., Frontoni, E., Gottardi, G., Sciarroni, D., & Spalazzi, L. (2017). Certificate Validation through Public Ledgers and blockchains. ITASEC, 156-165.
9. Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P., & Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renewable and Sustainable Energy Reviews, 100, 143-174. https://doi.org/10.1016/j.rser.2018.10.0
10. *Embark Framework by Status home page*. https://framework.embarklabs.io/docs/overview.html /
11. Ethereum Developer Resources. https://ethereum.org/en/developers/docs/smart-contracts/verifying/
12. Infura development suite , https://infura.io/
13. InterPlanetary File System , https://www.geeksforgeeks.org/interplanetary-file-system/

AUTHOR BIOGRAPHIES:

1. Erina Kiran Kumar ,MCA, M.Tech, Scientist-D, NIC, Meity, GOI, Vijayawada.
Areas of Interest: Cloud Computing, Block chain, data analytics, Big Data.
(ORCID:0000-0003-0390-0963)
2. Sanaboyina Madhusudhana Rao, B.E, MBA, Scientist – F, NIC, Meity, GoI,Vijayawada
(ORCID: 0000-0002-8389-5887)
Areas of Interest: Cloud Computing, Database Design, Block Chain Technology, AI, ML, Data Analytics
3. Vinay Sowpati, B.E, M.Tech, Scientist –C, NIC, Meity,GoI, Vijayawada (ORCID: 0000-0002-6551-1376)
4. Dr PVSS Gangadhar, PhD, Scientist-E, NIC, Meity,GoI, Vijayawada.(ORCID: 0000-0002-8548-8492)
Areas of Interest: Cloud Computing, Big Data, IoT, Fuzzy Logic, Security, e-Governance.