CertChain - Generic Certificate Chain Platform

A Concept Note

Center of Excellence in Blockchain Technology

National Informatics Centre

Bengaluru

Table of Contents

1. Introduction

Several documents issued by the government are essential for the citizens, especially for claiming benefits of various social welfare schemes, job and legal purposes and education admissions. These documents need to be stored safely and produced on demand to the authorities. Most of these documents are currently issued to citizens in a paper-based format even though the data is stored electronically. The paper-based format is subject to loss, fraud, theft, blurring of the print, etc and verifications of these documents takes long time. Hence there is a need for providing a fool-proof method that is digitalized and expeditious in obtaining and verifying the document.

To circumvent the above problems associated with paper-based documents, National Informatics Centre (NIC) has developed blockchain technology based solution called Cert Chain for secured storeage and retrieval of documents. The Cert Chain ensures that the documents are recorded securely in tamper-proof manner and easily traceable. The main advantage of this generic Cert Chain system is that the documents could be accessed online by any authorised person / institution and be assured that it is genuine and not tampered – all this without the need for an intermediary.

2. Challenges in the current systems

a) Fake documents

The use of fake documents to claim the benefits from various social welfare schemes has been prevalent for several decades. With the improvement in the technologies and internet, the generation of fake certificates has become even more rampant and easy for unscrupulous elements of society. Many times these fake certificates can have a detrimental effect on the government exchequer and, more so, depriving the benefits to the genuine beneficiaries.

b) Tonnes of paperwork

The process of obtaining a duplicate certificate involves a lot of paperwork, right from lodging a complaint with police, filling up a request form for a duplicate certificate, payment of fees, and of course, waiting for the concerned authority to retrieve the certificate from the record room and issue the duplicate certificate.

c) High cost

The cost of paper and printing itself is not the only item of expenditure related to documents. Major institutions and schools spend enormous amounts on storing this information.

d) Delay in verification

Ascertaining the authenticity of certificates issued by issuing institutions has become a major cause of concern these days due to the prevalence of malpractices like fraud and misrepresentation of records. This issue is further compounded with Issuing/verifying institutions collecting high fees, as well as entailing a long wait time for processing and verifying the certificates. The citizen needs to provide documentary proof of eligibility to avail of Government Services. Often, notarised documents / attested documents are to be submitted, which results in the out-of-pocket expenditure and requires losing a days' earnings. After it is submitted to the authorities, the verification of documents is a lengthy process which could be as simple as examining the original document produced by the application or as complex as sending the document to the issuer to ascertain if the document was indeed issued by that person.

e) Data can be changed, hacked or lost due to natural disasters

With data being stored in a centralized location, there are chances of the data being tampered in addition to be a single point of failure. The loss and damage to documents is quite a common basis for litigation, which results in financial costs and wasted time.

f) Need for carrying of original certificates to verify the authenticity

The students need to produce the original documents to various authorities for higher studies/employment etc. Loss or damage to these documents during travel is a cause for concern.

3. Cert Chain - The Novel Solution

The Cert Chain is developed using blockchain technology to record the data in a digital format. The system can store the documents and changes to them and link them like a chain. The Cert Chain records the information in a distributed manner across multiple locations. Tampering the information present in the chain is not possible as the document is stored in the blockchain after the consensus is obtained from all the peers to synchronize the data between them; thereby, ascertaining anti-tamper characteristics of the Cert Chain.

4. Benefits

The generic Cert Chain system developed using blockchain technology provides trustable, immutable, and traceable documents with quick access. It can be used by various organizations and departments of governments to store and as well as retrieve the document. The system can be used to store various documents like birth certificates, death certificate, caste certificates, income certificates, mark sheet, transfer certificate, etc. Certificates can be used by the various departments to sanction the social benefits to the concerned persons after verifying the documents and also could be used by other organisations such as insurance companies, educational institues etc, to verify the claims of the customer by clearly avoiding any intermediary.

Changes to the documents will also be submitted to the Cert Chain by the issuing authority. The Cert Chain system will then link these new updates of the documents and store them securely.

The system provides quick and reliable access for verification. This paperless-based system saves time for verification and promotes an electronic verification process.

The Generic Cert Chain developed enhances the following features.

- Transparency
- Tamper-proof
- Paperless
- Free from third-party interference.
- Trail of the certificates
- Single platform for enabling the storage and retrieval of different types of documents

5. Users of DocChain

The Cert Chain system provides a mechanism for the storage of documents issued by various departments called the issuing authority and retrieval of the documents by individuals/organizations and use it for providing services called the Consuming entities.

The system is a single platform that provides the issuing authority and consuming entities a standard procedure for storage and retrieval of any document issued by the government. The Cert Chain provides a mechanism for any agency to verify the details of the documents. It could help professional colleges, departments providing scholarships, hostel facilities, job providers and financial institutions to get the documents verified without the need for a third party. It also saves time for physical verification and promotes a paperless verification mechanism.

The following Departments / Agencies could be the users of the Cert Chain platform . Fig 1 gives the various stake holders of the Cert Chain Platform.

- Educational Institutions
- Govertment Departments
- Employers
- Students
- Financial Institutions

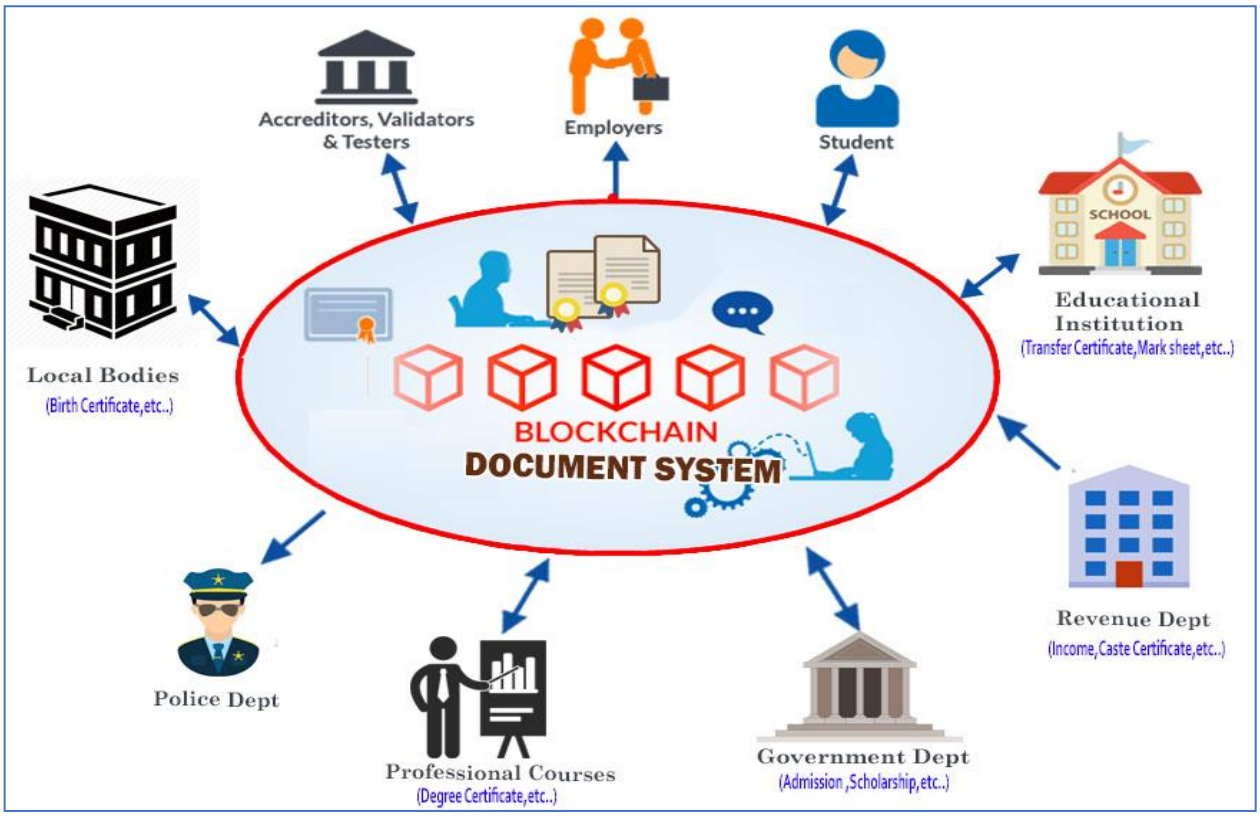

Fig 1.

6. Solution Architecture of DocChain

Various departments like registrar of Birth and death, Revenue, Commercial taxes, Sub-registrar offices, etc would be authorized to store the documents in the Cert Chain system; other stakeholders who act as consumers will be able to retrieve the certificates based on the authorization provided by the owners/ issuers of the documents. The on-boarding of the various stakeholders who would like to consume the data from the Cert Chain system or the use of API verification will be done by the portal. The architecture for facilitating these activities is given below in a pictorial form (Fig 2).

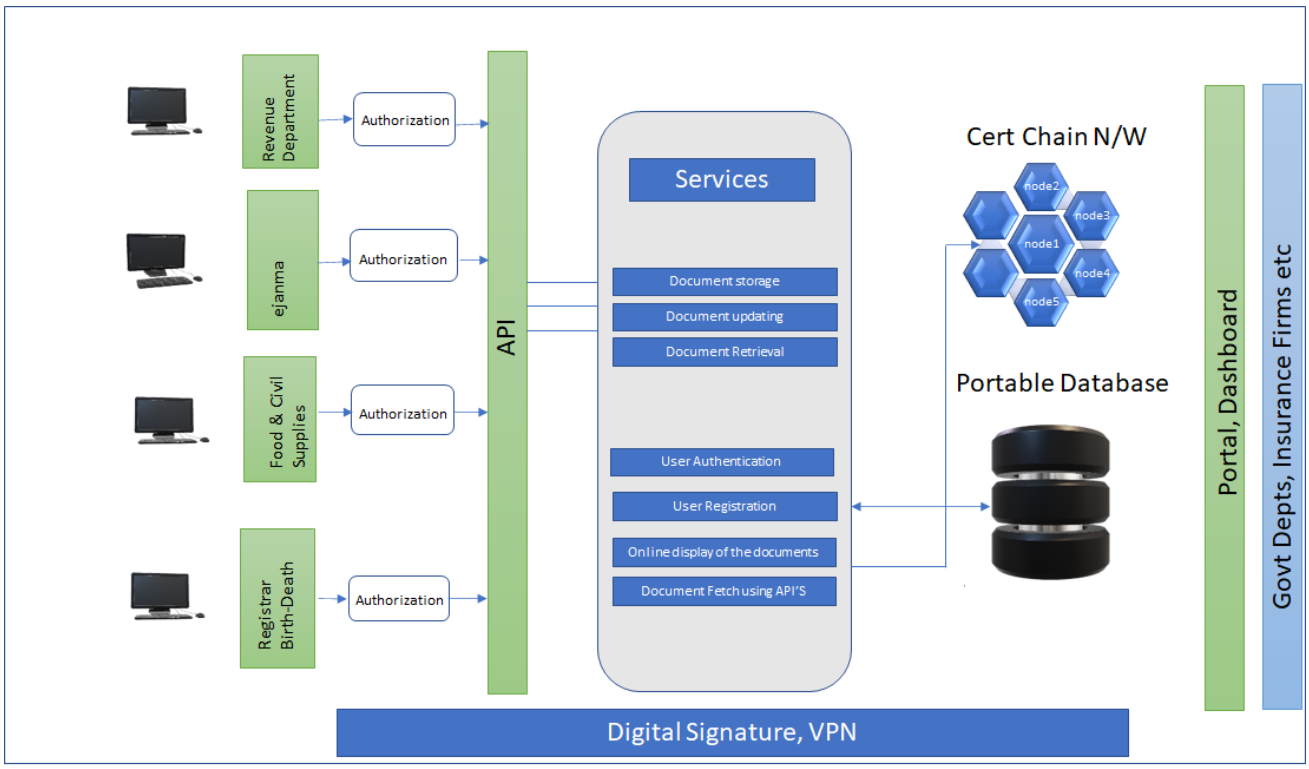

Fig 2.

The process of storing the documents in the blockchain will greatly aid as supplementary to the existing processes followed by various departments/offices, and organizations, etc. In computerized offices, the data is stored in the databases after the approval of the issuing authority. The existing processes will continue to work as before, except that the digitally signed documents will also be stored in the Blockchain by comsuming APIs provided for the purpose. The Cert Chain system will also record the changes made to the document, and the end-user will be able to view those changes.

7. Verification Methodologies

The Retrieval Process of documents/certificates from the Cert Chain system can be enabled with multiple methods. The process of verification depends upon the type of users – Citizens and Orginsations. The processes of verification could be Web portal, File upload and API. Web portal will be interactive wherein one-by-one document can be verified. The file upload involves the bulk document verification and API will help two IT system to exchange data in machine readable data and internally process accordingly.

8. Verification By Citizens

Citizen can verify the document by going into the Web portal. Verification by the citizens could be carried out using different methods – Based on document details or based on Aadhar number, provided aadhar number is stored with document, or based on blockchain ID.

9. Verification By Organisations

The orgnaisations can verify the document with multiple methods. The organisations need to register and follow the guidelines of the government for accessing the data. The verification process can be carried out by one of the following methods

- One-by-one verification on the portal. The orgnaisation can enter the details of the certificate such as the document type and the ID and the details will be displayed.
- Bulk Verification : The orgnaisation can upload a list of certificate IDs for which the document details are required to be verified. The portal will retrieve the document details from the blockchain and prepare a file that can be downloaded by the orgnaisation.
- API to integrate with the line of business application : The orgnaisation can use APIs to fetch the data from the Cert Chain and integrate it with his application so that the logic for automatic verification, updation can be built. This will help to automate their processes of verification.

10. Conclusion

The Cert Chain system is a blockchain-based platform to securely store and retrieve documents digitally. The verification of the claims by citizens for availing services of the government can be done electronically, thus reducing the time and the cost. Blockchain also provides the trust to assure the verifier of immutability of the documents. Rather than old hierarchical methodology, the technology becomes the focus, with the trust migrating towards the technology, not the institutions or departments, etc. Thus, this is a disintermediation technology.

ANNEXURE-I

What is Blockchain?

Blockchain is a technology protocol that enables data to be exchanged directly between different contracting parties within a network without the need for intermediaries.

Blockchain is a decentralized distributed database (ledger) of immutable records accessed by various business applications over the network. It is implemented on a peer-to-peer network of computers where in each computer is a called as a node. Nodes can be owned and maintained by the stakeholders who participate in the Government processes.

Client applications of related Government departments can read or append transaction records to the blockchain. Transaction records submitted to any node are validated and committed to the ledger database on all the nodes of blockchain network. Committed transactions are immutable because each transaction is linked with its previous block by means of hash and signature values. Consensus algorithms based on voting / leader selection / lottery and distribution ensure that the submitted transactions are transferred to all nodes and committed on all blockchain nodes consistently.

Blockchain technology would provide the necessary impetus to move from demand based process of service delivery to eligibility based system. With the citizen data created by various government departments on the blockchain and the eligibility criteria being agreed upon by all departments, it would be possible to achieve this. The 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.

Typical categories of applications that would see value from blockchain implementations are Identities, Registries,SupplyChain and License/ verifications / permits. Specifically, applications related to issue of certifiactes like caste / income / birth / death / Surviving Family Member / Land Records / Driving License etc and Supply Chain category of application such as Drug Logistics / State Excise Supply Chain / Agricultural Commodities supply etc would benefit from blockchain implementations.