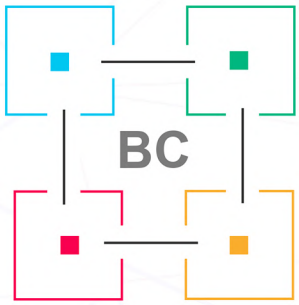
# Document Authentication Using BlockChain




## Problem Statement

Validating the authenticity of academic certificates of individuals is always an arduous task. It generally involves reaching out to the certificate authorizing bodies (e.g. Colleges/Universities/ Institutions) and following protocols, which are unlikely to be similar, to seek the information needed. Needless to say, it requires reasonable amount of time and effort to accomplish the ends.

## Solution

Blockchain can be applied to resolve the bottlenecks related to the delays, that are an intrinsic part of the process, by creating a repository of certificates. The process would involve storing the fingerprint of a given document, i.e. a certificate in this case, and some metadata related to it in the database. Subsequently, at any given point in time, the authenticity of a certificate can be determined by querying the blockchain using the fingerprint of that certificate and determining whether there exists in the database a similar document.

# Current Status quo/problem

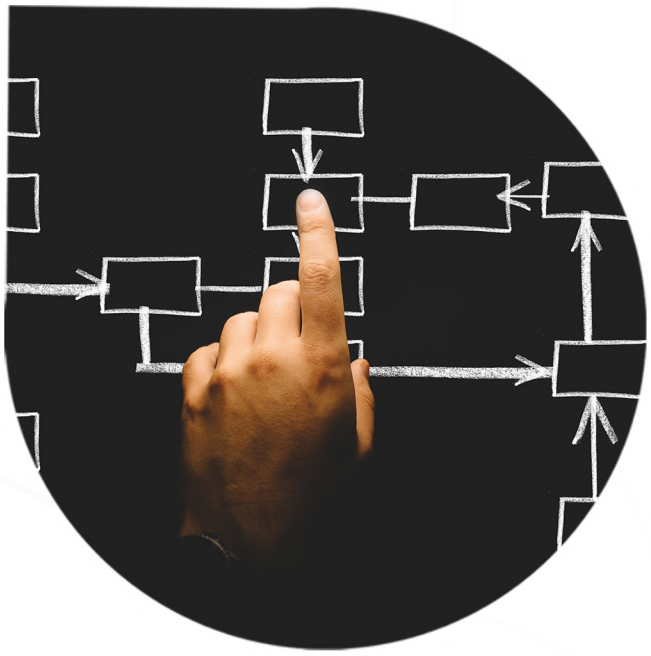
On successful completion of a course, an individual is issued a certificate of merit with details on grades and other relevant information by the authorized College affiliated to some University. The process is broadly similar whether it is a full time, part time or a vocational course. The individual is expected to produce the document in its original form every time he has to prove his credentials somewhere.

Now, verification of the certificate is a tricky affair, because an original certificate can be forged with some effort. So everytime there is a need, it is common norm to seek a response from the authorizing body in order to determine the authenticity of the certificate details shared. It being a complex and an arduous process, the services of third-party organizations who specialize in this field of work are availed. Needless to say, there is a cost and time involved in the process. Matters that require urgent responses suffer as a result.

# Solution

In general terms, a blockchain is an immutable transaction ledger, maintained within a distributed network of peer nodes. These nodes each maintain a copy of the ledger by applying transactions that have been validated by a consensus protocol, grouped into blocks that include a hash that bind each block to the preceding block. Let us now take a look at how the concept can be put to use in the current context.

All the organization issuing these certificates can form a consortium and keep uploading the original certificates (i.e certificate fingerprint and metadata) in the blockchain environment. Subsequently all the organizations/parties who want to validate the authenticity of the certificates will also need to join the same blockchain environment and depending upon need directly query using the fingerprint of the certificate to determine authenticity.



**Let us take an example to explain the above scenario:**

There are educational boards for school education that issue certificates to students who successfully complete their Grade 10 exams. Now these education boards can store the certificate fingerprints along with some metadata in a blockchain environment. For every student, the concerned educational board can provide the student with the corresponding fingerprint along with a digitally signed copy of the certificate (this is the copy whose fingerprint is stored in the blockchain).

Now, whenever the same student needs to submit the certificate to any organization that seeks it, he can just provide the fingerprint of the certificate and the respective organization can easily verify the authenticity by querying the blockchain using the fingerprint of the certificate. Or else, the student can provide the digitally signed certificate itself. Subsequently, the organization can generate the fingerprint of the certificate and directly query the blockchain for authenticity.

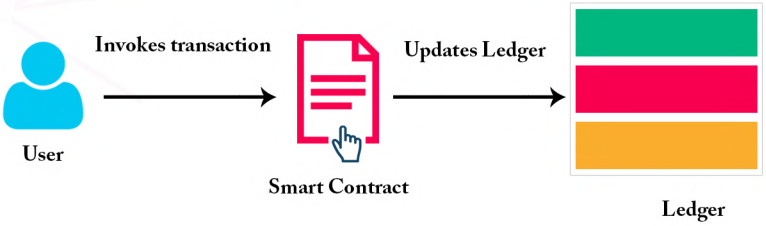
The main advantage with such a process is that we can eliminate any chances of fraud. Because, if anyone tampers the original certificate before submitting it, the fingerprint would change and will lead to an invalid certificate notification from the blockchain at the time of determining its authenticity.

# Technical implementation Details

- In the background it uses Hyperledger Fabric blockchain environment to store the information and NodeJs SDK to communicate with the Hyperledger Fabric.
- Main business logic to store the information resides in the blockchain as a chaincode written in NodeJs.
- Every time a student register/verifies a document, it invokes different functions of the chaincode. It is the chaincode which stores and retrieves the data in the blockchain.

# Chaincode

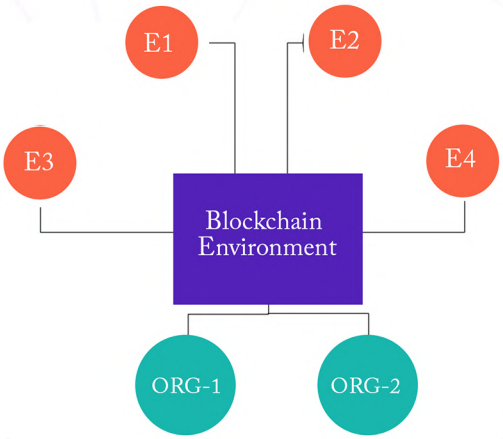
- Chaincode is a program written in Go, Java or Node Js which can read and update the ledger state. All the business logic is inside the chaincode.
- Chaincode implements the logic agreed upon by members of the blockchain network and so qualifies to be considered as a “Smart Contract”.
- Chaincode can be installed on one or more peers/nodes and instantiated on a channel.
- Chaincode runs in a secured Docker container isolated from the peer process. Ledger state cannot be updated directly by anyone in a Hyperledger Fabric application. It can only be modified by submitting transactions that calls different functions in a chaincode.
  So, any read or write operation has to be done through a chaincode.




When creating a chaincode, there are two methods that needs to be implemented.

- **Init**
  Called when a chaincode receives an instantiate or upgrade transaction. This is where application state is initialized.
- **Invoke**
  Called when the invoke transaction is received (query or update the ledger state).

# Blockchain Environment

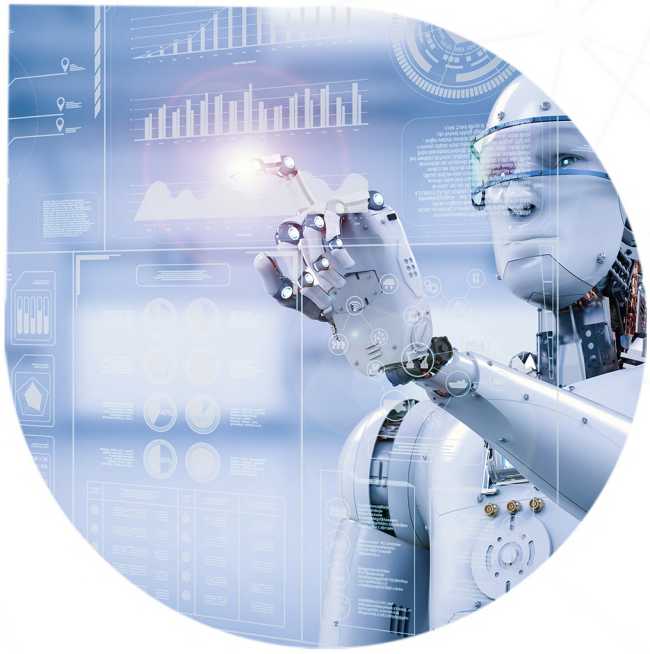



There are four Educational Institutions who have formed a consortium and agreed to store the Degree Certificates of their student in the Blockchain environment.

All the EIs(Educational Institute) can store and retrieve data from the Blockchain Environment.

Org1 and Org2 are the organisations who can query the data from the blockchain and validate the Authenticity of the certificate.

# True Decentralization



The chaincode governs the rules for any read/write operation on the Blockchain. The biggest benefit of using Blockchain to store sensitive data such as important documents is that chaincode can't be updated/modified even by the developers who initially built it unless consensus is reached by the participating organizations/members.

For example: 5 organizations decided to join the Blockchain consortium and initially they defined a rule that at least any 3 organization's approval is needed to update the chaincode. So, as long as any three organization doesn't put their signature in the updated chaincode transaction file, the chaincode can't be updated. So, it guarantees that read/write operation will never change.

The architecture that drives Blockchain takes away the privilege that a centralized database offers its users - that of an exclusive access. And so, in the process also eliminates possibilities of single rogue users mis-utilizing the prerogative. Bitcoin, the first application of Blockchain, for instance, has never been hacked till date; reflecting the impregnability of the system.