**Blockchain for Transcript Verification**

**Apoorva Dwivedi, Wishnoo**

**University of Massachusetts, Boston**

**ABSTRACT**

Blockchain technology enables the creation of a decentralized environment, where transactions and data are not under the control of any third-party organization. Any transaction ever completed is recorded in a public ledger in a verifiable and permanent way. Counterfeit academic certificates have been a longstanding issue in the academic community. Establishing a secure federated identification to confirm the identity of the issuing institution. Based on a globally distributed peer-to-peer network, it will first, generate the electronic file of a paper certificate accompanying other related data into the database, meanwhile calculate the electronic file for its hash value. Finally, store the hash value into the block in the chain system. The system will create a related QR-code and inquiry string code to affix to the paper certificate. It will provide the demand unit to verify the authenticity of the paper certificate through mobile phone scanning or website inquiries. Through the unmodifiable properties of the blockchain, the system not only enhances the credibility of various paper-based certificates, but also electronically reduces the loss risks of various types of certificates. The platform is a first step toward a more transparent and technologically advanced form of higher education systems

**INTRODUCTION**

Blockchain is a distributed database that is widely used for recording distinct transactions. It features a decentralized and incorruptible database that has high potential for a diverse range of uses once a consensus is reached among different nodes, the transaction is added to a block that already holds records of several transactions. Each block contains the hash value of its last counterpart for connection. All the blocks are connected and together they form a blockchain.  The proposed system will exploit the benefits of the blockchain, as a decentralized architecture, offering security, anonymity, longevity, integrity, transparency, immutability and global ecosystem simplification, in order to create a globally trusted higher education credit and grading system. As a proof of concept, we will present a prototype implementation of the platform.

# MOTIVATION

Academic credential fraud is reality and counterfeiting documents is a very colloquial problem and its getting easier day by day. On the other hand, averment of these documents is becoming cumbersome process for institutions and employers. The majority of higher education institutions (HEIs) keep their students’ completed course records in proprietary formats. These databases are structured to be exclusively accessed by an institution’s staff and in dedicated online systems, hence with little or no interoperability. Furthermore, the majority of institutions have their own specialized system for keeping students’ completed course records, which preserves the proprietary data structure of the database. There are several vital points in regard to such systems, including standardization of data, storage location, safety and how to filter, analyze and securely share such data. Hence, students can experience difficulties transferring to another HEI, while still preserving and proving their completeness of courses from the previous institution. This problem is even more vivid in cases when a student wants to transfer to another country, where a language, script and administrative barrier exist. Moreover, these records are usually stored in different standards, which make it difficult to exchange records between HEIs. In cases when the student applies for a job position and has to prove his/her academic degree in a foreign country, problems arise from the centralized storage of students’ complete course records due to their inaccessibility, lack of standardization, etc. The students have to translate and notify their academic certificate which can be a complex and time-consuming process

### OBJECTIVE

In this study, we developed a decentralized application and designed a certificate system based on Ethereum blockchain. This technology was selected because it is incorruptible, encrypted, and trackable and permits data synchronization. By integrating the features of blockchain, the system improves the efficiency operations at each stage. The system saves on paper, cuts management costs, prevents document forgery, and provides accurate and reliable information on digital certificates.

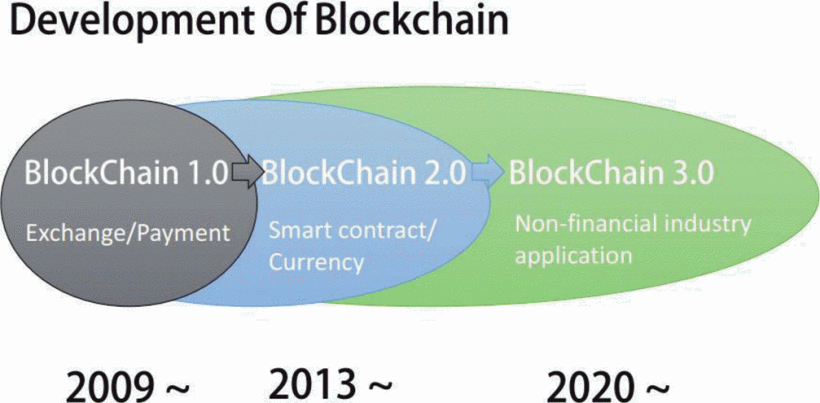
### CONTRIBUTION

In this project we have tried to implement a transparent process of verifying the transcript. Here the college will first verify the details of the student and then when verified, it will generate a QR code that can be placed on our CV’s and when we scan and view it with our key. It will show all the details about that student.

## LITERATURE REVIEW

### A. BLOCKCHAIN

The concept of blockchain was proposed by Satoshi Nakamoto in 2008. Blockchain is an online ledger that provides decentralized and transparent data sharing. With distributed recordings, all transaction data (stored in nodes) are compressed and added to different blocks. Data of various types are distributed in distinct blocks, enabling verifications to be made without the use of intermediaries. All the nodes then form a blockchain with timestamps. The data stored in each block can be verified simultaneously and become inalterable once entered. The whole process is open to the public, transparent, and secure .The emergence of Ethereum Smart Contracts in 2013 boosted blockchain technology, which became blockchain 2.0. As presented in Fig. 1, blockchain 1.0 was mainly adopted by Bitcoin to solve problems concerning cryptocurrencies and decentralized payments. Blockchain 2.0 focused on decentralizing the entire market and is employed to transform assets through smart contracts, thereby creating value through the emergence of alternatives to Bitcoin.



### B. ETHEREUM

### Ethereum is an open and decentralized platform featuring Turing completeness and supporting various derivative applications. Most smart contracts and decentralized autonomous organizations are created by using Ethereum .If the Bitcoin blockchains are considered a global payment network, Ethereum would be the global computing system. Furthermore, Ethereum is an open-source platform similar to Android (developed by Google). It provides an infrastructure that enables developers to create applications. The infrastructure is developed and maintained by both Ethereum and those developers. The major characteristics of Ethereum are as follows:

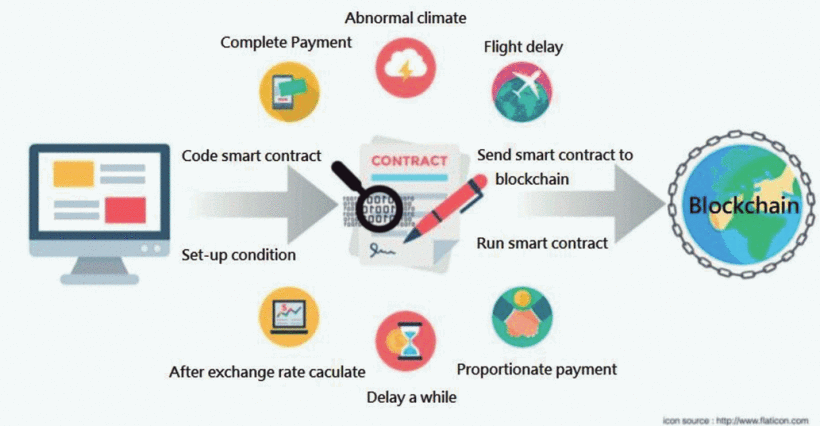
1. incorruptible: third-parties are not able to modify any data;
2. secure: errors derived from personnel factors are avoided because the decentralized applications are maintained by entities rather than individuals;
3. Permanent: blockchain does not cease to operate even if an individual computer or server crashes.

#### C. SOLIDITY

Solidity is the programing language used for implementing smart contracts and is similar to JavaScript. After a Solidity-programmed smart contract is completed, a complier called solc is required to transform the Solidity code into contract bytecode, which is then interpreted by the EVM. Next, the compiled instructions are deployed in an Ethereum blockchain. This completes the whole process

### D. SMART CONTRACTS

Smart contracts were first proposed by Nick Szabo in the early 1990s. He explained that a smart contract enabled computers to execute transaction clauses. As blockchain has become popular, smart contracts have received increased attention. Smart contracts are the main feature of Ethereum, a blockchain platform founded in 2015. A smart contract is “a digital contract that is written in source code and executed by computers, which integrates the tamper-proof mechanism of blockchain”. Smart contracts can be created using the Ethereum blockchain. Developers are able, according to their needs, to specify any instruction in smart contracts; develop various types of applications, including those that interact with other contracts; store data; and transfer Ethers. Additionally, smart contracts that are deployed in blockchains are copied to each node to prevent contract tampering. With related operations executed by computers and services provided by Ethereum, human error can be reduced to avoid disputes regarding such contracts. Smart contracts are mostly used in voting system and cryptocurrency applications. Fig. 3 depicts an example of how developers can easily deploy smart contracts for cryptocurrency transactions. The high-level programming languages used for writing smart contracts are mainly Solidity, Serpent, and LLL. Currently, most developers employ Solidity to write smart contracts and compile the instructions into bytecode for the EVM to execute. Certain costs are incurred when developers create smart contracts.



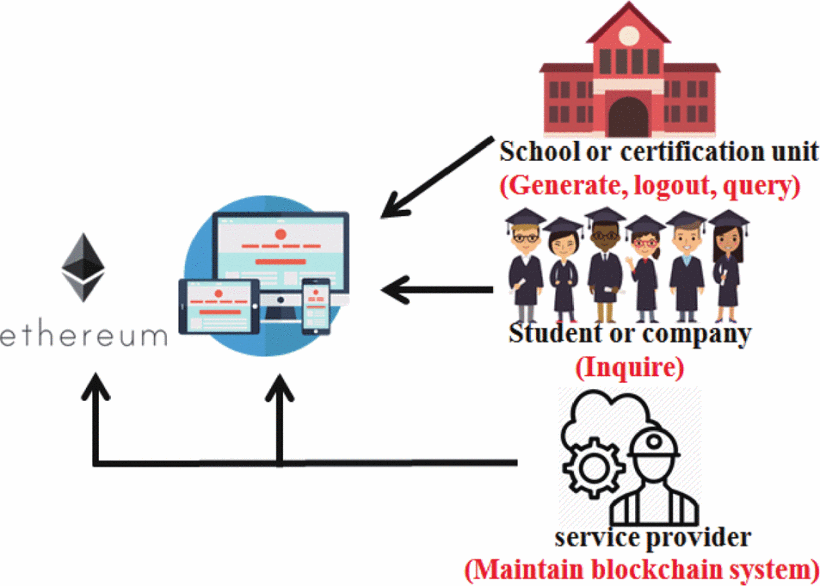
**D. IPFS**

IPFS is a peer-to-peer distributed file system that seeks to connect all computing devices with the same system of files.  IPFS provides a high-throughput, content-addressed block storage model, with content-addressed hyperlinks. IPFS seeks to create a permanent and distributed web. It does this by using a content-addressed system instead of HTTP’s location-based system. IPFS uses a representation of the content itself to address the content. This is done using a cryptographic hash on a file and that is used as the address. The hash represents a root object and other objects can be found in its path. Instead of talking to a server, you gain access to this “starting point” of data. This way the system leverages physical proximity.

## RESEARCH METHODS

### A.SYSTEM DESIGN

In this study, a blockchain certificate system was developed based on relevant technology. The system's application was programmed on the Ethereum platform and is run by the EVM. In the system, three groups of users are involved, (Fig. 4). Schools or certification units grant certificates, have access to the system, and can browse the system database. When students fulfilled certain requirements, the authorities grant a certificate through the system. After the students have received their certificate, they are able to inquire about any certificate they have gained. The service provider is responsible for system maintenance.



 The working processes of the system developed in this study are as follows:

1. Schools grant a degree certificate and enter the student's data into the system. Next, the system automatically records the serial number of the student in a blockchain.
2. The certificate system verifies all the data.
3. Instead of sending conventional hard copies, schools generates a quick response (QR) code to the graduates whose data have been successfully verified. Each graduate also receives an inquiry number.
4. When applying for a job, a graduate simply sends the serial number or can add the QR code to his/her CV and send it to the target companies.
5. The companies send inquiries to the system and are informed if the serial numbers are validated. The QR code enables them to recognize if the certificate has been tampered with or forged.

**CONCLUSION**

Data security is one of the major features of blockchain technology. Blockchain is a large and open-access online ledger in which each node saves and verifies the same data. Using the proposed blockchain-based system reduces the likelihood of certificate forgery. The process of certificate application and automated certificate granting are open and transparent in the system. Companies or organizations can thus inquire for information on any certificate from the system. In conclusion, the system assures information accuracy and security.

**References**

* Smart contracts whitepaper, [online] Available: https://github.com/OSE-Lab/learning-blockchain/blob/master/ethereum/smart-contracts.md.
* Blockchain and smart contract for digital certificate :Jiin-Chiou Cheng;Narn-Yih Lee;Chien Chi;Yi-Hua Chen
* Chris Dannen, Introducing Ethereum and Solidity, [online] Available: https://www.apress.com/br/book/9781484225349.
* Solidity, [online] Available: https://solidity.readthedocs.io/en/latest/index.html.
* A Blockchain-Based Higher Education Credit Platform : Muhamed Turkanović; Marko Hölbl; Kristjan Košič; Marjan Heričko; Aida Kamišalić