Deqree: Certificate Validation using Blockchain Technology

Written by:

Advait Joglekar

advaitjoglekar@yahoo.in

Adnan Khan

strangelet.lol@protonmail.ch

ABSTRACT

Deqree is designed to be a transparent yet secure method for degree and certificate validation using a public ledger that allows us a trustless way of authorizing and verifying certificate ownerships. Digital signatures are crucial for combating the problem of fake credentials and making verification easy. Institution issued records backed by entries in a decentralized blockchain make such certificates tamperproof and undisputable. In the case of academic qualifications, it is reasonable to conclude that (a) an academic qualification is a public transaction between an Institution and a student, (b) certain stakeholders need access to these transactions, and (c) each transaction cannot be changed once it has been completed. These assumptions are in conjunction with the decentralized existence of blockchain and the absence of the need for a trustworthy authority.

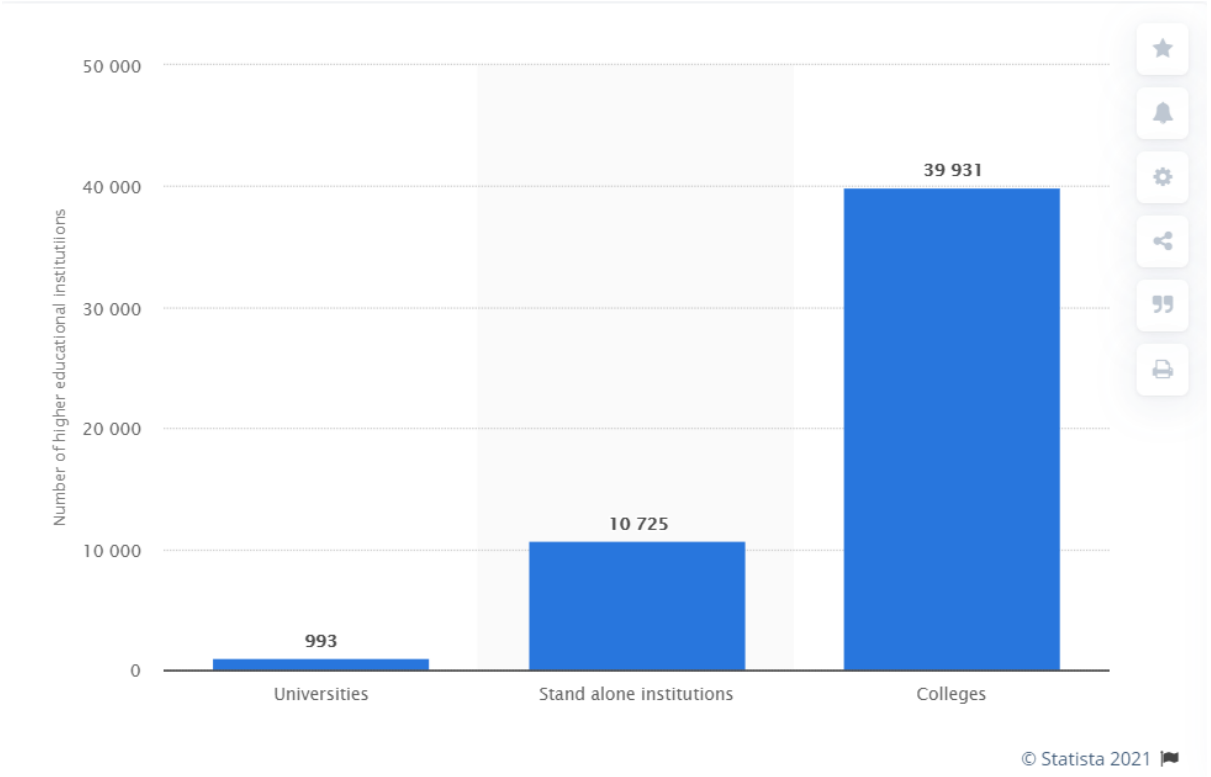
1. Introduction

The Indian higher education system is currently marred with several logistical flaws that have become necessary to be resolved after years of frustrating students and recruiters alike. The number of graduates is growing as the number of universities and tertiary education system grows. The method of verifying these degree certificates produces a lot of paperwork and if they are being stored digitally, it requires a central authority who is in control of maintaining the records which creates a possibility of tampering and data loss. Some academic institutions allow an easy and fast online query to check the validity of their credentials, without even asking who requires the information. Some delegate the task to third parties (either by design or by regulation) or market the service. Finally, there are occasions when there is little choice but to contact the academic secretary's office at the educational institution, so that one can confirm if a certificate or qualification is legitimate. Academic credential fraud, on the other hand, is a reality that occurs as a result of counterfeiting as well as the involvement of authorities' and institutional employees. According to the Centre for Educational Studies and Service (CESS), 15 lakh engineering graduates alone pass out every year in India.[5] In a huge crowd of graduates, verifying degrees is a crucial step in preventing fraud and establishing confidence in the applicant. However, degree verification has lagged behind technological advances and is often a time-consuming manual operation. 2 Ideally, it should be trivial for any organization to verify the claimed degree of an applicant. As long as it is not easy to do so, there are inefficiencies in the job-market, and higher educational-application process. As result, many companies bypass the verification process and rely solely on the applicant's term, creating fertile ground for fraud. In fact, a news article published in September 2020 discusses a few ways to spot a fake degree, and the methods mentioned clearly highlight the lack of a reliable and efficient way to do such a check.[3]

The lack of an electronical equivalent of an educational degree is the greatest impediment to automated verification. It will appear that converting a paper degree to an electronic one is easy. However, transferring a degree's authentication features, such as a signature, becomes extremely difficult without opening the door to the production of more fake degrees.

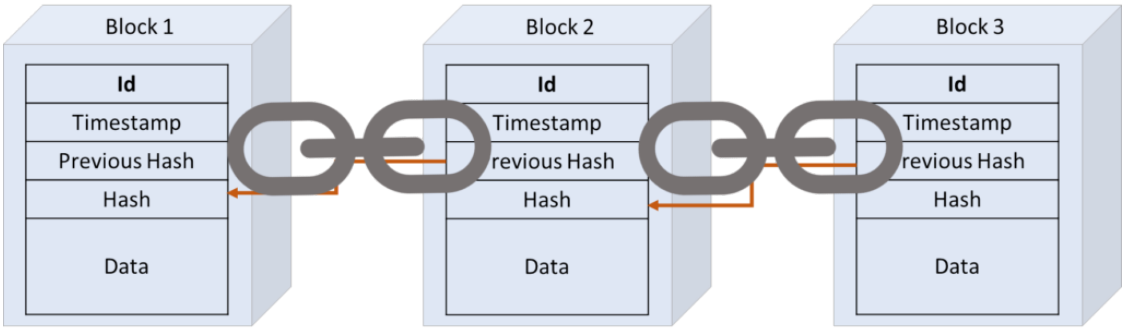
2. Present Situation

In today's India, with the youth making up to a whopping 1/3rd of the population, we indeed have a humongous education realm. Currently, India is a hub to over 51,000 higher education institutions which consists of over 37 million students across 993 universities, 39,931 colleges and 10,725 stand-alone institutions, according to the AISHE2019 studies. [6] While other studies show India's higher education enrollment having the commendable ability to jump from a mere 27% to 65% there is certainly an issue of concern.[7] India being a populous country, home to many youths, being a doorway to many educational opportunities, is lacking a fixed, secure, reliable, and tamper proof method to verify credentials. This problem is a serious drawback, as there are innumerable number of fraud cases, which degrades the velocity of our growing education sector along with the job markets. The current resources available today are not secure enough to limit frauds to a negligible number. They unfortunately have many loopholes and on top of that they fail to be cost effective. Having a proper, secure, and reliable system to verify credentials is the need of the hour.



3. Proposed Solution

It was about six years ago that a new generation of blockchain technology emerged that provided a smart contract functionality. This feature enabled developers to use the advantages of a decentralized ledger to create applications by themselves that relied on the benefits provided by such a system. Since blockchain technology is immune to data alteration by design, it can manage to provide significant aid in the verification of academic credentials. Blockchain is an open, distributed ledger that can securely and permanently record the transactions of an academic ecosystem efficiently and in a verifiably tamper-proof way. Because of the decentralized existence of blockchains, the date on which a particular information was registered(timestamp) cannot be modified and is publicly verifiable without



requiring to put faith or confidence in any third parties. The use of a decentralized public blockchain is a more straightforward, cost-effective, and 3 convenient solution. It requires no need to rely on a centralized authority to store the database and keep the hope that they do so securely without any corruption. Thus, using such an extremely reliable, quick, secure, and immutable technology will ensure the quality of graduates entering the job market in their respective fields. Supporting quick checking of degrees is also in the best interests of any alumni or degree holder. This inefficiency in the job application process causes prolonged waiting times for the applicants. Furthermore, in this digital era, the provision of a physical copy of the degree has become obsolete. As a result, a solution for automated verification for this ecosystem would benefit the Institution, the holder, and the verifier.

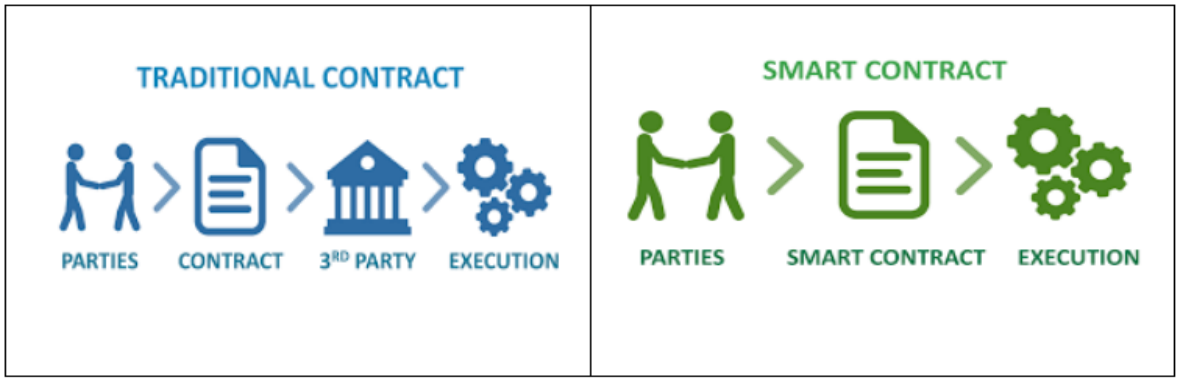
Hence such a system provides us with all the framework and tools needed to build a robust and secure application for our needs.

4. Cardano and Smart Contracts

Cardano is a project that began in 2015 as an effort to change the way cryptocurrencies are designed and developed. It aimed to take an unconventional way where it relied on publishing peer-reviewed research papers and then implementing it in code.

This has thus ended up making this blockchain a rigorously studied and tested project. This also makes it one of the main reasons why we have faith and plan to build on top of this blockchain.

In our daily lives, we enter into many different kinds of contracts. These contracts are agreements that involve an exchange of value. These agreements can range from simple to complex, from buying a morning coffee to signing a mortgage for a house. The basic idea of smart contracts is that many kinds of contractual clauses can be embedded in the hardware



and software that we deal with, in such a way as to make the breach of contract expensive for the breacher.[2] Cardano, the first third generation blockchain to evolve from a peer-reviewed philosophy, will soon launch its own smart contract platform, Plutus. The goal of Plutus is to model the widest range of contracts that exist in the world today in the form of digitally secure & programmable smart contracts.

Such functionality has been managed to be implemented with the help of blockchain technology. This ability empowers us to write programs and create autonomous contracts that can be utilized to create a system tailored for digitizing degree records in a transparent fashion.

5. Native Token

A token is a short term for “asset token”, which is the on-chain representation of an asset and its basic accounting unit. Some cryptocurrency ledgers have built-in support to track ownership and transfer of more than one type of asset. This type of Multi-Asset support is called native.[4] Cardano's Multi-Asset functionality is native.

Native tokens represent some value and act as an accounting unit, which can be used for payments and transactions. They can provide a unique utility for the purpose set by the creator. Without tokens, transactions and smart contracts will only see the amount of the blockchain’s native asset, without being able to see the purpose to which any asset may have been dedicated. On Cardano, anyone can create their own native token. This feature allows us to create our own token for the purpose of accountability and better traceability.

In Cardano, all native token transfer logic is coded in the ledger. This ensures the predictable and uniform behavior of the system. The native tokens share the same security ad ADA itself. On other platforms, such as Ethereum, the existing tokenization process requires custom codes that add to the complexity and security concerns. The tokens which are created using Smart contracts are non-native tokens. The underlying ledger does not support these tokens.This introduces another layer of complexity, expense (other chains need smart contracts to execute tokens), and inefficiency, as token code for both specifications is replicated and adapted instead of becoming part of the framework itself. It also allows for the possibility of human error. If custom code is written carelessly, it can introduce bugs that result in financial loss, which was the case in 2017, when software bugs resulted in the loss of $300 million in Ethereum cryptocurrency.

Cardano native tokens are set to change the current scenario. The solution allows tokens to behave similarly to Cardano's main currency, ada, allowing projects to take advantage of market-leading levels of speed and security while lowering costs.

6. Metadata

Metadata means "data about data". It is used to summarize basic information about data which can make tracking and working with specific data easier. Transaction metadata is a valuable feature for developers who build applications and process transactions, and for application end users. Developers embed metadata directly and submit a valid transaction with accompanying details. End users do not interact with the metadata directly but can view transaction-specific metadata using an Explorer. Transactions can contain metadata whose hash is part of the body of the transaction. Because the metadata hash is in the transaction body, this allows for integrity checking and authentication of the metadata.

Cardano provides us with the ability to add metadata to transactions executed on the blockchain. The data can be added directly, or, for larger amounts, it is possible to create a Merkle tree of the data and put the root hash of the Merkle tree on the blockchain. Once this is done, it can be proved that the data existed at a specific point of time and that it remains permanently on the chain for future reference.

The data that can be expressed through metadata are diverse, ranging from numerical data to strings, and many other things in between. In Cardano, the structure of the metadata is defined by a mapping from keys to values (key-value pairs) that combine details for multiple purposes into the same transaction. The metadata values are simple terms, consisting of integers, text strings, byte strings, lists, and maps. Values are required to be structured, which makes it easier to be inspected and managed, particularly by scripts. This feature gives us immense utility to store the data for our needs.

7. Conclusion

We have proposed a solution to verify certificate credentials without relying on any third party trust. The use of blockchain technology thus allows us to create a robust framework for immutable data storage that is independently and securely verifiable while also being easy to access. An application built on top of such a system will increase efficiency and significantly enhance the capabilities of Institutions not just in India but also all around the world to streamline verification of an individual's credentials.

References

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", https://bitcoin.org/bitcoin.pdf, 2008
[2] Nick Szabo, "Smart Contracts: Building Blocks for Digital Markets", Nick Szabo -- Smart Contracts: Building Blocks for Digital Markets (uva.nl), 1996
[3] How students and employers can spot and eliminate fake degrees, Education Today News (indiatoday.in)
[4] Multi-Asset Tokens Explainer
[5] Students keep IITs as backup, Deccan Chronicle
[6] A Study on Education Enrollment in India, Kritika Sharma, The Print
[7] India - higher education institutions by type 2019, Statista