

BLOCKCHAIN-ENABLED PLATFORM FOR FRAUD –RESISTANT DIGITAL CERTIFICATE AUTHENTICATION

Sarath P Biju

PG, Student

The Oxford College of Engineering,

Bommanahalli,

Bengaluru- 560068

sarath.p.biju333@gmail.com

Dharamvir

Associate Professor

Dept. of MCA

The Oxford College of Engineering, Bommanahalli,

Bengaluru- 560068

dhiruniit@theoxford.edu

ABSTRACT

A person's future can be significantly impacted by their college credentials. They assist people in showcasing their credentials or enable companies to confirm that a candidate has the abilities required for a specific position. Existing methods for confirming academic accomplishments are frequently cumbersome, costly, and susceptible to fraud, despite their crucial social significance.

Students can quickly and easily get a safe, verifiable copy of their certificates thanks to this project. The system also ensures the authenticity and integrity of the certificate while offering high security, durability, and convenience. We suggest applying blockchain technology to solve the certificate duplication issue. Since data on a blockchain cannot be altered, tampering is impossible because any updates or modifications necessitate the creation of a new block.

In order to fully utilize the potential of this technology, we want to promote cooperation amongst institutions and hasten the adoption of blockchain for digital certification.

Keywords: QR code, blockchain technology, digital certificates, safety, and education

INTRODUCTION

Students who successfully finish courses at different levels are awarded certificates by universities and other educational establishments. The electronic ones cannot fully substitute the physical ones which have traditionally been used as such certificates. The increase in fraudulent certificate creation has occurred due to the wide access availability of scanning and printing equipment by the relatively low cost technology that exists today. Both issuing organizations and holders of the certificates are affected by this problem. Verifying that a graduate's certificate is authentic and that the person presenting it is the legitimate owner is crucial.

Furthermore, to guarantee the legitimacy of the certificate's issuance as well as its authenticity, educational credentials must be validated. Traditional verification techniques are frequently expensive and time-consuming. On other hand, digital systems have the benefit of quick and effective certificate verification. We have

decided to investigate blockchain technology in order to successfully execute this concept.

Everyday life has changed dramatically as the result of the proliferation of digital data, widespread internet access, and widespread use of mobile devices. Due to the ease of digital transactions, virtual currencies—which were initially designed for online use—have gained popularity over time. Well-known cryptocurrencies like Bitcoin, Ethereum, and Ripple have grown in popularity and value. The underlying technology of these cryptocurrencies, blockchain, has gained attention as a result.

LITERATURE SURVEY

The Social Consequences of Blockchain

The potential of blockchain technology to decentralize systems and lessen dependency on specialized authorities has drawn a lot of interest from the media and academic community. Widespread blockchain adoption may have significant impacts on social structures, with both possible advantages and disadvantages. There is relatively little literature addressing the wider societal or The potential operational challenges that could crop up as a result of that path. blockchain integration, despite as the fact that are technical challenges have received as a lot of attention.

Overview of System Architecture

Creating a system blueprint are the first stage in creating blockchain-based solutions. The three

primary components of a typical system as nodes that store blockchain-related data is distributed, encrypted fashion, application providers that handle user data for operational or business purposes (e.g., targeted services or customized offerings), and mobile users who download and interact with applications. Businesses and providers can maintain recognizable profiles on the blockchain, enabling their identity and transactions to be reliably verified, even though users may continue to use pseudonyms.

EXISTING WORK

Traditional Certification Systems' Difficulties

Academic and professional certification administration has historically been centralized and largely done by hand. In a order to verify the authenticity of are the credentials, each verification takes a significant amount of work and involves several administrative procedures. Institutions find it challenging to react quickly to requests for verification because this procedure is frequently laborious and resource-intensive. When a lot of certificates need to be verified at once, the centralized approach puts a lot of strain on administrative staff and raises the possibility of mistakes or processing delays.

Support Services' Restrictions

Private organizations' support services, like those offered by banks or third-party verification agencies, haven't always been successful in overcoming these obstacles. For students or graduates, these are the systems frequently fall short in providing prompt or trustworthy verification. The procedure is still laborious and prone to delays even with this assistance, which may have an impact on applications for jobs, admission to universities, and other opportunities that depend on timely verification. The verification process is made more difficult by the absence of institutional integration and standard operating procedures.

PROPOSED SYSTEM

Certificate Digitization and Hashing

A conventional paper-based certificate is first transformed into an electronic record by the system, which then stores it in a secure database together with all associated metadata. A distinct cryptographic hash is calculated for the document after the electronic record is created. By serving as a digital fingerprint, this hash guarantees the certificate's integrity. After that, the hash is appended to a blockchain block, connecting the certificate to the decentralized ledger and

guarding against unwanted changes. This procedure keeps a direct link to the original paper version of each certificate while guaranteeing that it has a permanent, verifiable record.

Request strings and QR codes for validation

The system creates a request string code and a QR code for every certificate to improve security and accessibility. These tools make it possible for third parties, like employers or educational institutions, to quickly confirm the certificate's legitimacy. The verification unit can immediately determine whether the certificate is authentic by scanning the QR code or inputting the request string via a mobile device or website. Reliability is increased and administrative delays are greatly decreased by doing away with the need for manual verification.

Decentralized Integrity and Verification

Using a decentralized network of computers to validate the data is one of this system's most significant benefits. Transactions do not need to be manually confirmed, in contrast to conventional centralized methods.

METHODOLOGY

The system works efficiently to safely handle and validate student credentials. First and foremost, educational institutions are in charge of verifying students' degrees and entering their academic and personal data into the database. Following the entry of this data, each student is given a persistent ID by the system, which is then stored on a blockchain. Through the use of blockchain technology, the system makes sure that student data is safe and unchangeable, guarding against illegal changes or tampering.

Following data storage, each piece of information entered into the system is verified by the verification mechanism. Prior to the issuance of any digital certification, this underwriting procedure ensures the authenticity and correctness of student records. The system provides the integrity of the certification procedure with a close investigation of all the details ensuring that only genuine and substantiated credentials were added to the blockchain.

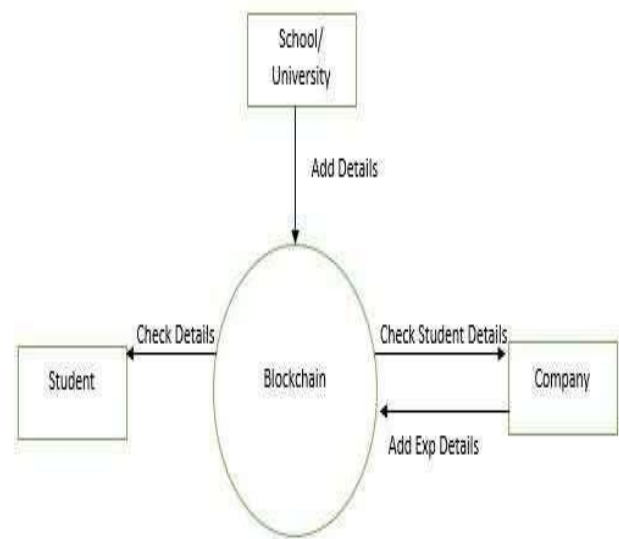


Figure 4.2.1 Context View1

A school first inputs the student's data into the system before issuing a certificate. Each student's unique serial number is automatically generated by the blockchain, guaranteeing a persistent and impenetrable identifier. After that, the school enters all of the student's data into the system, including both academic and personal information. An unchangeable record of the student's credentials is provided by the blockchain, where this data is safely stored. In order to preserve integrity and transparency, the school can also update the student's academic records, including exam scores, which are also stored on the blockchain. This are procedure guarantees that for all student data is correct, safe, and simple for authorized parties to verify.

EXPERIMENTAL RESULTS

accurately within reasonable time frames, and remains stable during intensive data processing or high use.

Unit testing is the process of assessing each system component separately to make sure it operates as intended. Using appropriate test data, each module is independently tested, and the outcomes are compared to what was anticipated. Before the smallest parts of the system are combined with larger parts, this procedure, also known as module testing, makes sure they function as intended.

Validation testing confirms that the program satisfies end users' requirements and expectations. That to make a sure the in system works as intended, it is tested in circumstances that are comparable to real-world use. A successful validation verifies that the program satisfies its functional specifications.

Integration are testing looks at the interactions between various modules. Individual modules are grouped into tiny groups after unit testing, and data flows between modules are examined to identify interface problems. This guarantees that the integrated modules function properly together and that any mistakes relating to interactions are found early on in the development process.

Acceptance testing the last stage prior to the system being put on operational use. It does not use simulated data, rather than the real data provided by the customer. This stage undergoes validation of whether the system meets business requirements and is ready to face the real business world.

In testing the integrated system, what is tested is whether the integrated system meets the criteria. To make sure that the accuracy and proficiency of the system, it simulates the life that might happen in the real world. In the testing of a process, process diagrams and data flow are also employed to ensure that tasks are accomplished in the right way and that all elements involved in the results are synchronized.

This methodical approach to testing guarantees the system's dependability, functionality, and security, giving users assurance that it will work as intended in a real-world setting.

Performance testing looks at how well the system can manage anticipated workloads. It guarantees that the program handles requests effectively, answers

CONCLUSION

Real world application Developers are now focusing more on data security. In essence, block chain are huge, dispersed, open online database in which every node involved stores and validates a significant quantity of data. Because each item is cryptographically connected and validated by many nodes, this decentralized structure significantly lowers the possibility of data tampering or fabrication.

This quality marks the fact that the information storage and validation process in the proposed blockchain-based system is secure, transparent, and credible. Each and every transaction or data entry made; be it a record of a student, academic credentials, or even corporate experience details are all validated automatically before they can be uploaded to the blockchain. This improves the integrity of the stored data by making the system very resistant to fraud or unauthorized changes.

Additionally, the system is designed to be transparent and accessible, enabling businesses, colleges, and approved organizations to get pertinent data as needed. As one example, an employer can use a QR code to access blockchain data regarding a student credential or

work experience information, with assurance of authenticity without intermediaries.

REFERENCES

- [1] Tengyu Yu, Analysis of the principle of block chain operation: 5 major technologies, iThome, <https://www.ithome.com.tw/news/105374>
- [2] Jingyuan Gao, The emergence of virtual currencies! Bitcoin is the first mover and the other 4 types can not be ignored. Digital Age, bnext.com.tw/article/47456/bitcoin-ether-li-tecoin-ripple-differences-between-cryptocurrencies
- [3] Smart contracts whitepaper, <https://github.com/OSE-Lab/learning-blockchain/blob/master/ethereum/smart-contracts.md>
- [4] Gong Chen, Development and Application of Smart Contracts, <https://www.fisc.com.tw/Upload/b0499306-1905-4531-888a-2bc4c1ddb391/TC/9005.pdf>
- [5] Several national junior diplomas will be launched next year, exempted as they will be of the cumbersome auditing and issuance processes. <https://www.ithome.com.tw/news/119252>