Applied GIS

ISSN: 1832-5505
Vol-4 Issue-01 Jan 2016

Smart Contracts: Digital Certificate-Based Document Verification on the Blockchain

Mansi Dandgaval1, Prachi Alex2, Sayali Tapkir3, Snehal Jadhav, Prof.Akash Dodke5
Computer Department, Indira College of Engineering and Management,
Savitribai Phule University, Pune, India

Abstract— The use of blockchain technology is one method for ensuring the integrity and authenticity of transactions involving sensitive information.Since each block in a blockchain includes a cryptographic hash of the prior block, a timestamp, and transaction data, we suggest a system where digital certificates are used for blockchain-based document verification.Therefore, the system not only improves the trustworthiness of paper-based certificates, but also minimizes the risk of loss associated with different kinds of certificates when transacted online.This aids in avoiding Certificate and Marksheet fraud while applying for jobs or enrolling in school.In addition, our system displays the current verification status of the applicant's submitted certificate of eligibility.

Keywords— Certificate Validation and Verification, Digital Certificates, Certificate Revocation, and the Blockchain

INTRODUCTION

By Providing False Documentation,The term "resume fraud" or "application fraud" is used to describe the practice of providing false, exaggerated, or otherwise misleading information on a job application or resume in order to increase one's chances of being hired for a position for which one is unqualified.It is anticipated that 26.5 million Indians will enroll in a postsecondary institution in 2014–15, with 9 million going on to get degrees.Indian higher education is vast and complicated, with over 20 million students enrolled in its 700 institutions and 35,000 associated colleges. The storage and organization of outcomes is the primary cause of the clumsy structure of degree-granting institutions. Some students will continue their education in another country, at their high school, or at a college or university, while others will be prepared to join the workforce. When applying to colleges or jobs, a student's academic credentials (such as certifications, transcripts, degrees, etc.) may be a huge selling point.

When schools issue certificates or degrees, all that has to be entered are the students' and institutions' names. The absence of a reliable anti-forge system means that incidents leading to a falsified diploma usually come to light. The digital certificate system built on blockchain technology is offered as a solution to the issue of certificate forgery. The block chain is a distributed, immutable database with potentially many applications.

Transactions may be recorded in a distributed ledger called a block chain. The digital certificate with anti-counterfeit and verifiability features was made possible by the immutable nature of blockchain. This system's digital certificate is issued in accordance with the following procedure:

Create the digital version of the paper certificate and enter it, along with any other relevant data, into the database. Finally, the hash value is recorded in the block of the distributed ledger. A QR code and an accompanying query string will be generated by the system and printed on the paper certificate. The requirement unit may then use their mobile device or a website to confirm the paper certificate's legitimacy. The solution not only improves the legitimacy of different paper-based certificates thanks to the immutable qualities of the blockchain, but it also decreases the loss risks of various certifications electronically.The certificate he/she has supplied for verification reveals the state in which the certificate is now located. Candidates and the companies they're interested in working for both have the option of establishing their own criteria for applying for certificate verification.

1.PROBLEM DEFINITION

When designing a smart contract, we set out to eliminate the possibility of fraud caused by phony certificates, as well as to make the process of acquiring and using such certificates more transparent and secure.We use Blockchain, a distributed database technology that operates as a "open ledger" to record and monitor transactions, to disclose the revocation status to the firm requiring and the applicant asking for verification of the papers submitted. Thus, it is necessary to provide an application where students may receive the entire paperwork like E- certificate with QR Code, making it simple for businesses, schools, and students to spot any cases of academic dishonesty. We built a blockchain-based certificate system and distributed application. Because of its transparency, security, and ability to synchronize data, this technology was chosen. The system's efficiency is enhanced throughout by using block chain capabilities. The solution is paperless, saves money on administration, prevents document counterfeiting, and delivers trustworthy data on digital certificates.

LITERATURE REVIEW

2.1.Background Study of Research Paper 1:

Ze Wang, Jingqiang Lin,Quanwei Cai,Qiongxiao Wang,Jiwu Jing and Daren Zha,"Blockchain based Certificate Transparency and Revocation Transparency"

This paper propose to record certificates and revocation status information in the global certificate blockchain, which is inherently append-only, to achieve certificate transparency and limited-grained revocation

ISSN: 1832-5505
Vol-4 Issue-01 Jan 2016

transparency. It balances the absolute authority of CAs, and provides a continuous history of certificates for each SSL/TLS web server. The certificates in log servers are organized as a Merkle hash tree. The system provides delegated certificate validation services for browsers- the prototype system with Firefox and Nginx.It introduces reasonable overheads in terms of storage, certificate validation delay.Its drawback is it Focuses on security of limited browsers.The publication of certificate is also publicly accountable.

2.2 Background Study of Research Paper 2:

Murat Yasin Kubilay,Mehmet Sabir Kiraz and Haci Ali Mantar,"CertLedger:A New PKI Model with Certificate Transperancy Based on Blockchain"

The CertLedger works on TLS CErtificates and PKI(public key infrastructure) architecture for Certificate Transperncy and Certificate Validation .It has more focus over the security of the Certificates from the attacks .Provides resistence from split-world attack.Drawback of the system is the revocation status is available to all and CertLedger cannot be implemented in exsisting blockchain framework

2.3 Background Study of Research Paper 3:

Pawel Szalachowski Stephanos Matsumoto Adrian Perrig,"PoliCert:Secure and Flexible TLS Certificate Management"

PoliCert proposes a comprehensive log-base and domain-oriented architecture that enhances the security of PKI by offering a stronger authentication of a domain's public keys, comprehensive and clean mechanisms for certificate manage-ment, and an incentivised incremental deployment plan. It doesnt work on TLS hence avoids TLS related error handling and client/server misconfiguration. Focuses only on preventing the MitM(Man in The Middle) Attack.

SYSTEM ARCHITECTURE

The issuing applications are responsible for the main business logic which includes the certificates applying, examining, verifying the document and issuing. The issuing applications are designed to merge the hash of the certificate in a hash table and send the hash table to Block-chain amidst signing by the majority of community members. Also, the issuing applications involved the revocation of certificate.

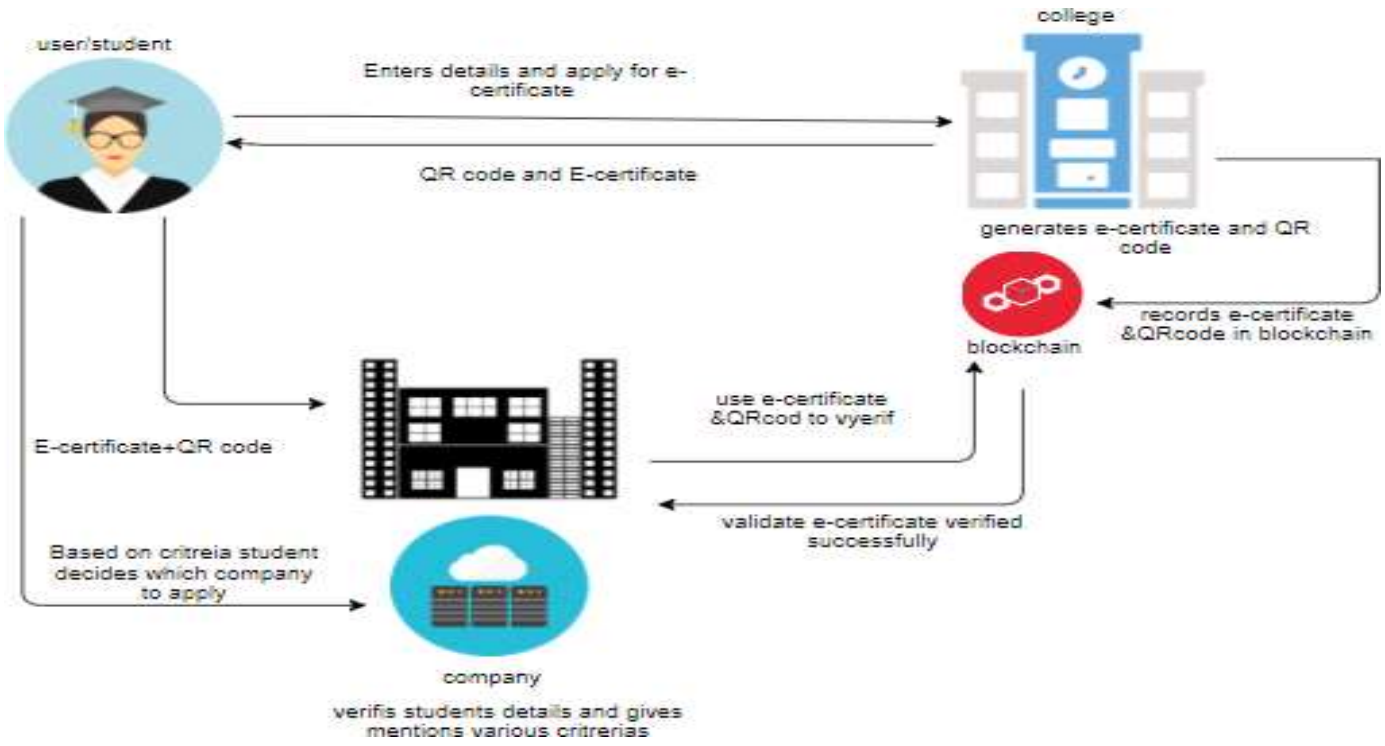

Fig.1 System architecture

ISSN: 1832-5505
Vol-4 Issue-01 Jan 2016

The student enters his personal details and gives it to college .The college generates a E-certificate and QR code containing his academic as well as personal details and saves the details in block-chain as well as gives the E-certificate and QR code to the student through the mail.Whenever the student wants to apply for any verification process or any company, instead of providing hard copies he provides his e-Certificate and QR code to the company .She/He doesn't need to carry all his certificates and details.The company verifies all the data with the block-chain whether the correct data is given. The QR code enables them to recognize if the certificate has been tampered with or forged.The company decides some criteria and based on the criteria details the student decides which company to apply.The verification application focuses on checking the authenticity and integrity of the certificates that have been issued. The mechanism can be briefly described in the following way:

- check the authentication
- code is valid check the hash with the local certificate
- confirm the hash
- ensure the hash value is in the block-chain
- verify the certificate

Also, it has to be mentioned that for the convenience of sharing the certificates, this application allows for verification of the documents by scanning the QR code directly.The block-chain acts as the infrastructure of trust and a distributed database forsaving the authentication data.Typically, the authentication data consist of the hash value generated using hashed data from thousands of certificates

FEATURES

1. Proposed an innovative solution to verify a certificate which is more reliable.
2. Utilizing multi-signature rather than the single private key makes the academic certificates issuing progress more secure. 3.The authentication data of the credential which published to block-chain is immutable, trustful and verifiable.
4.The new approach of authenticating the certificate (scan the QR code) simplified the workflow to efficient and economical. 5.The core data of the credential is secure and private even the block-chain technology crashes in the future.
6. Provides the status of Certificate Validation and Certificate Verification at each Phase

CONCLUSION

Thus, we have developed a system where the company is able to verify and validate the documents of the student or his/her employee or the candidates those have applied for a job using blockchain technology which keeps the documents safe, secure and provide a trustworthy way for the company to get the true or correct record of certificate.Including status at every phase of the system for document verification and transactions of digital certificates. This has in turn improved the performance of the system and assured more accuracy as well as security of information.With the increased implementation of Blockchain the system will be able to provide numerous features in addition to that of in existing system.

REFERENCES

[1] Ze Wang, Jingqiang Lin,Quanwei Cai,Qiongxiao Wang,Jiwu Jing and Daren Zha, *"Blockchain based CertificateTransparency and Revocation Transparency"*

[2] Murat Yasin Kubilay,Mehmet Sabir Kiraz and Haci Ali Mantar,*"CertLedger:A New PKI Model with CertificateTransperancy Based on Blockchain"*

[3] Pawel Szalachowski Stephanos Matsumoto Adrian Perrig,*"PoliCert:Secure and Flexible TLS Certificate Management"*

[4] Arvind Ramchandran, Dr.Murat Kantarcioglu,*"Using blockchain and smart contracts for secure data provenance management"*

[5] Xiuping Lin,*"Semi-centralized Block chain Smart Contracts: Centralized Verification and Smart Computing underChains in the Ethereum Block chain"*

[6] Yong Shi,*"Secure storage service of electronic ballot system based on block chain algorithm"*

[7] Zhenzhi Qiu, *"Digital certificate for a painting based on blockchain technology "*