International Journal of Computer Trends and Technology
ISSN: 2231-2803 / https://doi.org/10.14445/22312803/IJCTT-V68I3P114

Volume 68 Issue 3, 70-73, March 2020
© 2020 Seventh Sense Research Group®

Original Article

E-Certificate Generation Using Blockchain

Ebin Mathew[1], Maria Paulson[2], Reshma Joy[3], Jisha P Abraham[4]

[123]Department of Computer Science and Engineering, Mar Athanasius College of Engineering, Kothamangalam, Kerala, India
[4]Professor, Department of Computer Science and Engineering, Mar Athanasius College of Engineering, Kothamangalam, Kerala, India

Received Date: 14 February 2020
Revised Date: 26 March 2020
Accepted Date: 29 March 2020

Abstract *- In order to solve the problem of forged certificates, the digital certificate system based on blockchain technology would be proposed. By the immutable property of Blockchain, the digital certificate with anti-counterfeit and verifiability could be made. During education, the students achieve many certifications. While applying for jobs, students produce these certificates, where these are verified manually. There can be incidents where students may produce a fake certificate, and it is difficult to identify them. This problem of fake academic certificates has been a longstanding issue in the academic community. It is possible to create such certificates at a low cost, and the process to verify them is very complex. This problem can be solved by generating digital certificates on the Blockchain. Blockchain technology provides immutability and publicly verifiable transactions. These properties of Blockchain can be used to generate the digital certificate, which is anti-counterfeit and easy to verify. It is because the generated digital certificate cannot be edited or modified since it is generated through Blockchain, which makes it unchangeable.*

Keywords *- Blockchain, Hyperledger, Digital Certificate, Hashing.*

I. INTRODUCTION

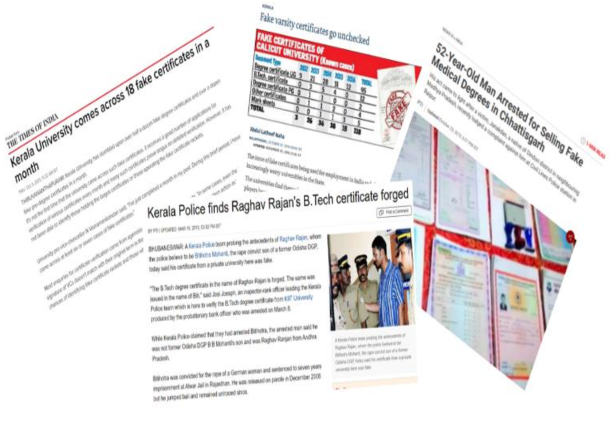
A. Background Information

Blockchain provides a decentralized and incorruptible database that has a high potential for a diverse range of uses. It is a distributed network that can have millions of users all over the world. It is a peer-to-peer(P2P) network where users can create unchangeable records and transactions. It can only be updated once it receives the consensus of all the participants in that network and is also known as the write-once, append-many technology. Every user can add information to the Blockchain, and all data in the Blockchain is secured through cryptography. Data in a ledger of transactions form a block. That block has an impact on the next block through cryptographic hashing. When a block is completed, it creates a unique hash code, which is tied into the next block creating a chain of blocks. A verified piece of data forms a block which then has to be inserted into the chain. The data it contains exists on the network permanently, meaning that it cannot be altered or removed. A public blockchain has ledgers that are managed autonomously to exchange information. A private or permissioned ledger to centrally administer their own transactions that can be used inter or intra-company. It is not hackable. The network of nodes must first agree that the transaction is valid. If someone hacks a computer system, then all the computer systems need to be hacked.

B. Rationale

Because information technology has developed rapidly in recent years, data protection is more necessary than ever. Tampering with data has been a serious threat these days. There have been many cases registered recently regarding fake certificates, as shown in Fig. 1.

To solve this problem, a certificate system based on Blockchain was designed in this study. The Blockchain provides a perfect system for the storage of information, be it static in the form of registry or dynamic in the form of transactions, registration and distribution. These data are recorded in an array sequence to one another, so altering one data will require altering all the historical records on every single node, which makes it immutable. Thus, the system is highly reliable.



THE TIMES OF INDIA

Kerala University comes across 18 fake certificates in a month

Fake varsity certificates go unchecked

FAKE CERTIFICATES OF CALICUT UNIVERSITY (Known cases)

Document Type	2012	2013	2014	2015	2016	TOTAL
Degree certificate UG	3	21	28	31	12	95
B.Tech. certificate	0	3	5	4	0	12
Degree certificate PG	0	1	1	0	0	2
Other certificates	0	1	1	2	0	4
Mark sheets	0	0	1	1	3	5
TOTAL	3	26	36	38	15	118

Abdul Latheef Naha

The issue of fake certificates being used for employment in India ... increasingly worry universities in the State.

52-Year-Old Man Arrested for Selling Fake Medical Degrees in Chhattisgarh

His act came to light after a victim, Janakilal, a native of Dindori district in neighbouring Madhya Pradesh, recently lodged a complaint against him at Civil Lines Police station in Raipur.

Kerala Police finds Raghav Rajan's B.Tech certificate forged

BY PTI | UPDATED: MAR 16, 2013, 03:52 PM IST

BHUBANESWAR: A Kerala Police team probing the antecedents of Raghav Rajan, whom the police believe to be Bibhotra Mohanti, the rape convict son of a former Odisha DGP, today said his certificate from a private university here was fake.

"The B.Tech degree certificate in the name of Raghav Rajan is forged. The same was issued in the name of Bibi," said Josi Joseph, an inspector-rank officer leading the Kerala Police team which is here to verify the B.Tech degree certificate from KIIT University produced by the probationary bank officer who was arrested on March 6.

While Kerala Police claimed that they had arrested Bibhotra, the arrested man said he was not former Odisha DGP B B Mohanti's son and was Raghav Rajan from Andhra Pradesh.

Bibhotra was convicted for the rape of a German woman and sentenced to seven years imprisonment at Alwar Jail in Rajasthan. He was released on parole in December 2006 but he jumped bail and remained untraced since.

Fig. 1 Cases on forged certificates (Courtesy:- https://timesofindia.indiatimes.com/home/education/news/Kerala-University-comes-across-18-fake-certificates-in-a-month/articleshow/23446738.cms)

C. Objectives

We developed a decentralized application and designed a certificate system based on 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 of operations at each stage. The system saves on paper, cuts management costs, prevents document forgery, and provides accurate and reliable information on digital certificates.

II. LITERATURE REVIEW

A. Blockchain

The concept of Blockchain was proposed by Satoshi Nakamoto in 2008. Blockchain can be explained as a growing list of records called blocks. Each block in a blockchain contains a cryptographic hash of the previous block, data and a timestamp. The data in Blockchain is tamper-proof. It is an open distributed ledger that records data in a permanent and verifiable way. Blockchain is managed by a peer-to-peer network adhering to a protocol for internode communication and validating new blocks. Once the data is recorded in a block, it can't be altered without the alteration of all successive blocks in Blockchain, which requires the permission of the network majority. Blockchain can be used in digital identity, tokenization, financial markets, inter-organizational data management and many more.

Blockchain is an online ledger that lends decentralized and transparent data sharing. Data of various types are distributed in distinct blocks, enabling verifications to be made without the use of intermediaries. All the blocks then form a blockchain with timestamps. The whole procedure is open to the public, transparent, and secure.

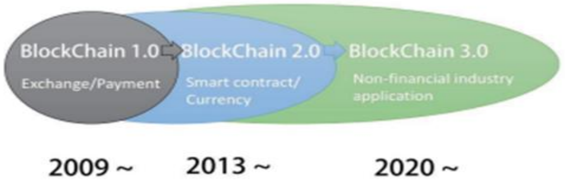


Fig. 2 Development of blockchain(Courtesy: https://ieeexplore.ieee.org/document/8394455)

As shown in Fig. 2, blockchain 1.0 was mainly adopted by Bitcoin to solve problems concerning cryptocurrencies and decentralized payments. Bitcoin is a digital and global money system currency. It allows people to send and receive money across the internet, even to the ones they don't know or don't trust. Money can be exchanged without being linked to a real identity. One of the differences between using bitcoin and using regular online money is that bitcoin can be used without having an internet connection to link any sort of real-world identity to it. Unless someone links their name to a bitcoin address, it is hard to tell the owner of the address. Bitcoin does not keep track of users or identities; it keeps track of addresses where the money is. Blockchain 2.0 focuses on decentralizing the entire market and is aimed to transform assets through smart contracts, thereby creating value through the introduction of alternatives to Bitcoin.

B. Hyperledger

Hyperledger is an umbrella project of open-source blockchains and related tools to support the collaborative development of blockchain-based distributed ledgers. Hyperledger Fabric is an open-source enterprise-grade permissioned distributed ledger technology (DLT) platform. It delivers some key differentiating capabilities over other popular distributed ledger or blockchain platforms.

The Fabric has a highly modular and configurable architecture. The beauty of modular architecture is that we can replace or add any one component without affecting the rest of the system. Therefore, it enables innovation, versatility and optimization for a broad range of industry use cases. These include banking, finance, insurance, healthcare, human resources, education, supply chain and even digital music delivery. For example, the Hyperledger Fabric must provide all participants on a supply chain network the ability to input and track sourcing of raw materials, record parts manufacturing telemetry, track the provenance of goods through shipping, and maintain immutable records of all aspects of the production and storage of finished goods through to sale and afterwards.

Fabric is the first distributed ledger platform to support smart contracts authored in general-purpose programming languages such as Java, Go and Node.js. The required skill sets needed to develop smart contracts are already present in the industries, and no additional training is needed to learn a new language.

The Fabric platform is also permission which implies that, unlike the public permissionless network, the participants are known to each other rather than anonymous and therefore fully untrusted. Permissioned blockchains can be seen as an additional blockchain security system, as they maintain an access control layer to allow certain actions to be performed only by certain identifiable participants. These are also different from private blockchains, which allow only known nodes to participate in the network. For example, a bank may be running a private blockchain operated through a designated number of nodes internal to the bank. In contrast, permissioned blockchains may allow anyone to join a network once their identity and role are defined.

Fabric can leverage consensus protocols that do not require a native cryptocurrency to incent costly mining or to fuel smart contract execution. As cryptocurrency is not involved in Hyperledger Fabric, it reduces attack factors. Since mining operations are absent, platforms can be deployed with minimal operational costs.

The combination of these differentiating design features makes Fabric one of the better performing platforms available today both in terms of transaction processing and transaction confirmation latency, and it enables privacy and confidentiality of transactions and the smart contracts (what Fabric calls “chaincode”) that implement them.

C. Smart Contracts

Smart contracts were first proposed by Nick Szabo in the early 1990s. He explained that a smart contract facilitated computers to execute transaction clauses. 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 that are deployed in blockchains are copied to each node. This is to prevent contract tampering. 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.

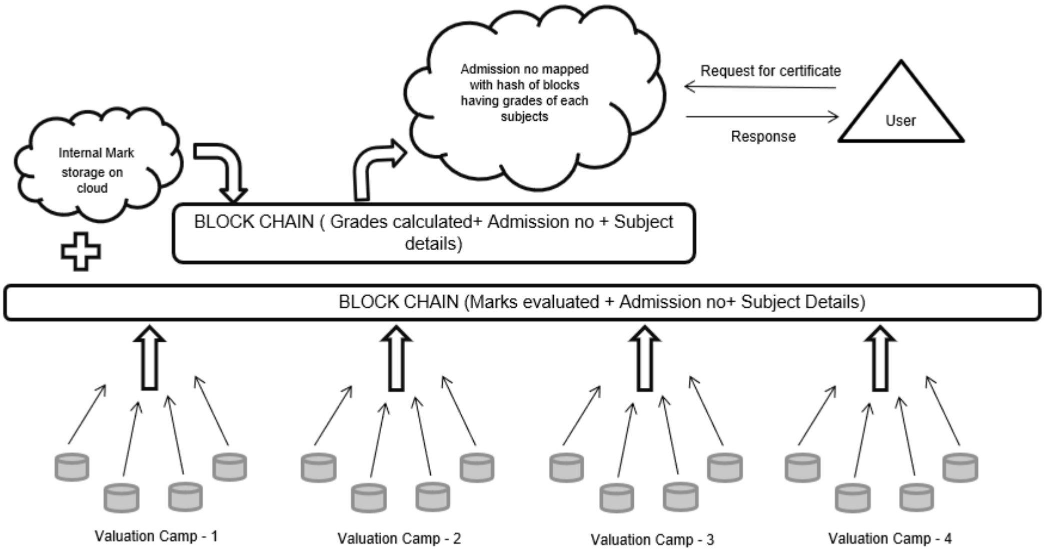

Admission no mapped with hash of blocks having grades of each subjects
Request for certificate
Response
User
Internal Mark storage on cloud
BLOCK CHAIN (Grades calculated+ Admission no + Subject details)
BLOCK CHAIN (Marks evaluated + Admission no+ Subject Details)
Valuation Camp - 1
Valuation Camp - 2
Valuation Camp - 3
Valuation Camp - 4

Fig. 1 Proposed System Design

D. Go Programming Language

Go is a compiled language, and hence it runs directly with the OS. This can allow us to build technology like EVM (Ethereum Virtual Machine) in a much better way. The Queries per second (QPS) is much better in Go than Java. Hence, it can be used to build systems to handle high volumes of requests.

Go was designed to improve programming productivity in multicore, networked machines and large codebases. The useful characteristics are static typing and run-time efficiency, readability and usability, high-performance networking and multiprocessing.

Concurrency is the ability to run several programs or several parts of a program asynchronously or in parallel, which improves the throughput. In Go, methods called Goroutines are used. Goroutines are methods or functions that can run with other functions in parallel. Blockchain has the wide importance of parallel actions. The ability to run a lot of functions in parallel allows programs written in Go to be run on distributed systems which is a primary need of blockchain technology.

III. DESIGN

A. System Design

A blockchain certificate system is developed based on relevant technology. The system’s application is programmed on the Hyperledger platform. In the system, valuators from different valuation camps enter the data, which consists of the mark and barcode, into the Blockchain. The barcode contains an Alphanumeric combination to uniquely identify each student. Based on the conditions specified in the smart contract, a student’s grade is determined from the marks and stored in the node.

B. Process

Certificate generation can be done using Blockchain by creating blocks of data of students that contain parameters such as Name, Admission number, Semester, Grades, Exam type. When a data entry operator enters marks of a student, a block is created with a hash value calculated from the mark. Likewise, blocks are created for each mark in a chain format. Suppose someone tries to tamper with the data, the hash value changes and consequently, the chain breaks. Therefore, data cannot be accessed by other blocks, and the nodes will come to know about the node that tampered with the data. So, the security of the system is ensured.

IV. RESULT

Using Blockchain for securing university evaluations has been implemented. Go programming language has been used to create the block containing each student's mark, subject code and the false number, which corresponds to each subject code for a particular admission number (unknown to evaluator). When this data in a block is modified by any person, its hash value changes, and so it is notified to every other evaluator, making it tamper-proof. The data in the Blockchain is fetched to generate the certificate of each student. If data has been modified in the certificate generated, it can be verified by retrieving the data from Blockchain using a QR code.

REFERENCES

[1] Jiin-Chiou Cheng, Narn-Yih Lee, Chien Chi, and Yi-Hua Chen, Blockchain and Smart Contract for Digital Certificate, Proceedings of IEEE International Conference on Applied System Innovation ., (2018).

[2] Neethu Gopal and Vani V Prakash, Survey on Blockchain-Based Digital Certificate System, International Research Journal of Engineering and Technology (IRJET), 5(11) (2018).

[3] Hyperledger Fabric, Available: https://www.hyperledger.org/projects/fabric/