

Blockchain Technology: Application in Notary Office

Karan Dalu, Prof. Sangram Dandge

Computer Science and Engineering, Prof. Ram Meghe College of Engineering and Research, Badnera

Abstract – The Notary office is responsible for issuing a variety of important certificates, but still uses manual processes and relies on paper documents from other government agencies. India is a developing country. Going digital is one of the crucial steps in the development of India, and this manual process causes a slew of problems. Non-local paper materials are rejected by the Notarial Office due to their reduced credibility in the local area, and as a result, cross-border services are unavailable. Because copies of paper items have been stored, it is also easy to leak sensitive information. And with increase in pollution, the usage of paper increases the strain on the Mother Nature. This is where need of block chain arises. In this paper, an online notarial application based on block chain technology has been presented. Eclipse platform, in which users will be able to send application for any document generation to notary admin, has been used. The notary admin will verify all the documents and process it. The documents sent will be encrypted by SHA 256 algorithm and the documents will be saved using the Inter Planetary File System (IPFS). This will improve security of documents and transparency of the process. The customer gets fast and the cost-effective services. The paper also includes, introduction to Block chain technology, its advantages, drawbacks, different types and how blocks are secured.

Key Words: Notary office, Blockchain Technology, Personal data Storage (PDS) SHA 256, Inter Planetary File System (IPFS)

1. INTRODUCTION

Currently most of the established organizations (e.g., hospitals, universities, banks etc.) use web enabled systems to provide their services and host their clients' data. Recently, online social networks (e.g., Facebook, Twitter, and LinkedIn) have revolutionized the individual's attitude towards data sharing. Individuals (e.g., data subject) now want to share their personal information such as academic record, and medical records with others (e.g., data consumer). They wish to provide others secure and selective access to their personal data hosted at different data-custodian systems (which stores and manage individual's data) for different purposes. However, different data custodians have different goals and policies related to the individual data subject's access to.

Traditional organizations (e.g., university, hospital) are usually reluctant to allow their users to share their data outside of their administrative domain. In some cases,

they outsource the limited sharing functionalities to a trusted third party (e.g., universities in Australia and New Zealand have outsourced academic record sharing to a third-party organization called My eQuals. The following are some of the reasons for organizations not to allow the data subjects to share their data [4]:

- i) There are legal implications for possible sharing of data, so entities that possess data tend to keep them locked
- ii) Data (and the knowledge related to them) represent a useful and valuable good, thus companies do not intend to share information with others
- iii) The lack of sharing facilities from data custodians has fueled the recent popularity of cloud based Personal Health Record (PHR) [5] and Personal Data Storage (PDS) solutions among the data subjects

Personal Data Storage (PDS) service providers provide cryptographic solutions to store encrypted data to ensure the confidentiality of the personal data on the cloud. They allow the data subject to store their data from different data custodians (e.g., health data, academic data etc.) in a single place. It helps the data subjects to get a "subject-centric" view of their data. However, in PDS-based system, the shared data is not being accessed directly from the source/issuing authority; data consumer has to often rely on offline notarization mechanism to proof the authenticity of the shared document. Sometime, data consumer (the shared party) communicates back to the data generating organization (e.g., Employers call back to the university to validate academic certificate of a student). This is often time consuming and inefficient. Therefore, we need a system where data consumer can easily verify the authenticity of the shared document.

Residents in numerous nations rely on government certifications on a daily basis. On the other side, citizens' faith in government erodes due to a lack of transparency, excessive bureaucracy, and even instances of corruption. The Notary Office has most official certifications to establish estate ownership, familial links, death, and so on. The purpose of creating a Notary Office is to standardize the certification process, minimize the number of certificate papers, and improve certification validity and acceptance. To produce a specific certificate, the Notary Office requires documents signed by other government offices. The current notary process is under the manual handling and we are trying to bring that manual handling process on to the digital platform where people can apply for different certificates from

their home and no need to visit physically in any Notary office.

Block chains are distributed record that allows participants to interact with one another in a safe, irreversible manner without the use of middlemen and block chain-based system has a high level of availability and transparency. In addition, to secure personal sensitive information, a symmetric encryption function has been included to encrypt user personal data and prevent from data misuse. On the other hand, we feel that the design provided can be used to a wide range of government sectors.

The objectives of the proposed research work were as follows:

- To develop an online block chain based system for notarial office
- To implement Advanced Encryption Standards (AES) algorithm for document encryption
- To develop Interplanetary File System (IPFS) server for document storage

2. Block Chain Technology

Blockchain is a distributed database solution that maintains a continuously growing list of data records that are confirmed by the nodes participating in it [6]. The data is recorded in a public ledger, including information of every transaction ever completed. Blockchain is a decentralized solution which does not require any third party organization in the middle. The information about every transaction ever completed in Blockchain is shared and available to all nodes. This attribute makes the system more transparent than centralized transactions involving a third party. In addition, the nodes in Blockchain are all anonymous, which makes it more secure for other nodes to confirm the transactions. Bitcoin was the first application that introduced Blockchain technology. Bitcoin created a decentralized environment for cryptocurrency, where the participants can buy and exchange goods with digital money.

Blockchain as a technology has the potential to change the way how transactions are conducted in everyday life [1, 3 and 4]. In addition, the applications of Blockchain are not limited to cryptocurrencies, but the technology could be possibly applied in various environments where some forms of transactions are done.

3. Challenges and Limitations

Blockchain technology has some technical challenges and limitations [1, 8] which are as follows:

i) **Throughput:** The potential throughput of issues in the Bitcoin network is currently maximized to 7tps (transactions per second). Other transaction processing networks are VISA (2,000tps) and Twitter (5,000tps). As the frequency of transactions in Blockchain increases

to similar level, the throughput of the Blockchain network needs to be improved.

ii) **Latency:** To create sufficient security for a Bitcoin transaction block, it takes currently roughly 10 minutes to complete one transaction. This makes latency a big issue in Blockchain currently. To complete a transaction e.g. in VISA takes only a few seconds, which is a huge advantage compared to Blockchain.

iii) **Size and bandwidth:** The Bitcoin community assumes that the size of one block is 1MB, and a block is created every ten minutes [10]. Therefore, there is a limitation in the number of transactions that can be handled (on average 500 transactions in one block) [11]. If the Blockchain needs to control more transactions, the size and bandwidth issues have to be solved.

iv) **Security:** The current Blockchain has a possibility of a 51% attack. To overcome this issue, more research on security is necessary.

v) **Wasted resources:** The waste in Bitcoin is caused by the Proof-of-Work effort. There are some alternatives in industry fields, such as proof-of-stake. With Proof-of-Work, the probability of mining a block depends on the work done by the miner [12]. The issue with wasted resources needs to be solved to have more efficient mining in Blockchain.

vi) **Usability:** The Bitcoin API for developing services is difficult to use. There is a need to develop a more developer-friendly API for Blockchain.

vii) **Versioning, hard forks, multiple chains:** A small chain that consists of a small number of nodes has a higher possibility of a 51% attack. Another issue emerges when chains are split for administrative or versioning purposes.

4. Applications of Blockchain

Blockchain Technology was first time successfully implemented by Bitcoin for crypto-currency. To fully utilize this technology a lot of research is in process. Its applications can be grouped into two categories: Financial and Non-financial. Table: 1 shows the various applications of Blockchain Technology [2, 6, 8, and 9]

Table 1: Applications of Blockchain Technology

Sr.	Non-Financial	Financial
1	Notary public	Crypto-currencies
2	Music industry	Securities issuance, trading and settlement
3	Decentralized internet of things	Insurance Claims and Processing
4	Internet applications	Global Payments
5	Decentralized proof of existence of documents	Blockchain Government
6	Patents	
7	E-voting System	
8	Internet of Things (IoT)	
9	Cyber-security	

5. Problem Description

The Notary Offices are regional offices and are present in every city; these offices contain confidential information of the residents of those respective cities. And as these offices are not digitalized this important information is easily leaked, also even if a resident has moved out of the city he has to again visit the city physically for generation of the required certificate, here the need for the Online Notary Office arises which will digitalize the notary offices saving a lot of paperwork and also keep the documents secure.

5.1 Methodology

This section discusses the development process involved in developing the Student Gateway Record System, includes problem identification, proposed solutions and development technologies

A) Problem Identification

The problems are identified and mentioned below.

1. The current notary offices are in offline mode and if an individual needs any certificate he has to personally visit the regional office.
2. All the documents are in the form of pages because of this the confidentiality and security of documents cannot be completely maintained, and also use of paper harms mother earth due to cutting of trees.

3. If an individual has shifted from his hometown he has to come back to his hometown for any certificates.
4. The transparency regarding the completion of process is not known to the applicant.
5. Long queue in crowded regions leading to a lot of wastage of time for every individual

B) Proposed Solution

Developed an online notary office with the help of java web applications and clever cloud database which will help the residents of the country to use the services of notary office from anywhere in the world. This will reduce the duration of application process, the documents will be secure and the mother earth will also be unharmed as use of paper will be lessened. The documents will be secured with the help the Block chain technology in which the data is stored in the form of blocks. The encryption of data is done using the AES algorithm and the generation of hash value is done using the SHA 256 algorithm.

The following software was used to develop the solution:

- Eclipse
- MySQL workbench
- Python
- Java jdk
- Vs code
- XAMPP
- Clevercloud

6. Phases of the project:

Phase 1:

In first phase, users will be able to register in this system. Admin will register city wise notary offices. Notary city wise admins will be able to verify pending applications of users and process applications.

Phase 2:

In this phase, users will upload their documents on IPFS server. We have built one python IPFS server on which we are encrypting the documents using AES algorithm. The encrypted document will stored on IPFS server and details about the documents will be maintained in IPFS database in the form of blocks. All details will be stored in database in encrypted format using AES algorithm.

Phase 3:

In third phase, users will post new applications and submit documents required for the applications to city admin. The applications details will be

maintained on block chain server1 and block chain server2.

Phase 4:

In fourth phase, city admin will view documents submitted by user and check application form. If verified city admin will upload certificate. The certificate will be stored in encrypted format on IPFS server and transaction details will be maintained on block chain servers in distributed manner.

9. Michael Nofer et al. Blockchain, Bus. Inf. Syst. Eng 59(3) (2019)

CONCLUSIONS

The Blockchain technology is identified as the efficient and secured solution for handling Notary Office applications which compromises of confidential personal data.

ACKNOWLEDGEMENT

We would like to express our sincere gratitude to the Notary Office, Amravati for their assistance and support in understanding the current working process of the Office.

REFERENCES

- 1. Stef an K. Johansen:** A Comprehensive Literature Review On The Blockchain As A Technological Enabler For Innovation, Mannheim University, Department of Information Systems Nov. 2017
- 2. Dr. Michael Gebert:** Application of Blockchain Technology in Crowd funding: A Case Study, New European March 20 17
- 3. Dr. Eric G. Krause et al.:** Blockchain Technology and the Financial Services Market, White Paper- Infosys Sept., 20 17
- 4.** A beginner's guide to blockchain technology by Blockgeeks: <https://blockgeeks.com/guides/what-is-blockchain-technology>
- 5. Dr. Gareth R.T. White , Kev in Brown:** Future Applications Of Blockchain: Toward A Value Based Society , INCITE Conference, Amity University, India, October 2016
- 6. Danda B Rawat et al.** Blockchain Technology: Emerging Applications and Use Cases for Secure and Trustworthy Smart Systems, Journal of Cyber security and Privacy (Nov.2020)
- 7. Min Xu et al.:** A Systematic Review of Blockchain, Financial Innovations (2019)
- 8. Shweta Singh et al.** A Detailed Study of Blockchain: Changing the World, Int. Journal of Applied Engineering Research, Vol.13, No. 14(2018) pp 11532-11539.