|  |  |  |  |
| --- | --- | --- | --- |
| HIGH LEVEL DESIGN DOCUMENT  Document Verification Using Blockchain  UE19CS390A – Capstone Project Phase – 1  ***Submitted by:***   |  |  | | --- | --- | | **Atul Anurag**  **Danish Hashmi**  **Reyyala Chethan**  **Sahitya Sagiraju** | **PES2UG19CS075**  **PES2UG19CS101**  **PES2UG19CS325**  **PES2UG19CS349** |   Under the guidance of   |  | | --- | | **Dr. Sarasvathi V.**  PES University |   **January - May 2022**  **DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**  FACULTY OF ENGINEERING  **PES UNIVERSITY**  (Established under Karnataka Act No. 16 of 2013)  Electronic City, Hosur Road, Bengaluru – 560 100, Karnataka, India |

TABLE OF CONTENTS

|  |  |
| --- | --- |
| 1. Introduction | 4 |
| 1. Current System | 4 |
| 1. Design Considerations | 4 |
| 3.1 Design Goals | 4 |
| 3.2 Architecture Choices | 4 |
| 3.3 Constraints, Assumptions and Dependencies | 4 |
| 1. High Level System Design | 5 |
| 1. Design Description | 5 |
| * 1. Master Class Diagram | 6 |
| 5.2 Reusability Considerations | 6 |
| 1. ER Diagram / Swimlane Diagram / State Diagram | 6 |
| 1. User Interface Diagrams | 6 |
| 1. Report Layouts | 6 |
| 1. External Interfaces | 7 |
| 1. Packaging and Deployment Diagram | 7 |
| 1. Help | 7 |
| 1. Design Details | 7 |
| 12.1 Novelty | 7 |
| 12.2 Innovativeness | 7 |
| 12.3 Interoperability | 7 |
| 12.4 Performance | 7 |
| 12.5 Security | 7 |
| 12.6 Reliability | 7 |
| 12.7 Maintainability | 7 |
| 12.8 Portability | 7 |
| 12.9 Legacy to Modernization | 7 |
| 12.10 Reusability | 7 |
| 12.11 Application Compatibility | 7 |
| 12.12 Resource Utilization | 7 |
| Appendix A: Definitions, Acronyms and Abbreviations | 8 |
| Appendix B: References | 8 |
| Appendix C: Record of Change History | 8 |
| Appendix D: Traceability Matrix | 8 |

# Note:

|  |  |
| --- | --- |
| **Section – 1 & Section 2** | **Common for Product Based and Research Projects** |
| **Section 3 to Section 11** | **High-Level Design for Product Based Projects.** |
| **Section 12** | **High-Level Design for Research Projects.** |
| **Appendix** | **Provide details appropriately** |

# Introduction

The flow of our system will consist of a Certificate issuer who will generate certificates and those certificates will be validated by a panel within that organization before being sent to a student. Each certificate will have a unique hash key which can be used to validate the authenticity of the certificate by any organization through the portal. The benefit of such a system is that the student also faces less risk of losing or damaging a certificate and the validation of the certificate can also be done quite easily.

# Current System

The current system of storing documents is largely based on traditional database software which can be manipulated, changed, or deleted hence compromising the integrity of the document. There are some Blockchain based data storing solutions as well which use Proof of Work as their consensus algorithm which requires vast computational resources. Therefore, our proposed system uses Blockchain along with IPFS with Proof of Authority as our consensus algorithm to tackle this issue thereby easing the process of document verification.

1. **Design Considerations** 
   1. **Design Goals**

Our proposed system uses Blockchain which is very well known for its immutability and security. What happens is the document uploaded is divided into smaller chunks which are then cryptographically hashed and stored into the peer-to-peer network of nodes by the IPFS (Inter Planetary File System). The combined hash of all these hashes is then stored into the Blockchain with a consensus forming via the Proof of Authority algorithm. The main advantages of our system are that it maintains the integrity of the document, data is stored based on a p2p network, hence chances of data loss and data compromising is very less, and the last important advantage is that we do not require any heavy computational machinery to add a block or put up any high stakes as well. It uses a simple yet secure PoA algorithm to mine a block, cutting the usage cost exponentially.

* 1. **Architecture Choices**

Hybrid Architecture: Hybrid blockchains are blockchains that are controlled by a single organization, but with some permissionless processes. In this, anyone can view the blockchain but does not have access to mine a block or be a part of consensus and validators.

Pros:

Transparent handling of transactions- Anyone can see that a block is being mined but they will not be part of the consensus.

Reduced costs in mining a block. - The miners do not need to compete with each other since they belong to a single organization, hence an algorithm which requires less computational power can be implemented easily.

Less chances of malicious nodes. - Since all the entites belong the the single organisation, their identity will be known to them, hence there is extremely less chance of a node becoming malicious.

Cons:

Biased towards being centralized- Since the mining is being done only by the trusted sources of the orgainisation, it can be categorised as being centralised. However, since the blockchain is publically available for anyone to see, it resembles a decentralised structure as well.

Organization can manipulate the data- As the blocks are being mined by the organisation, any high-level authority can force the miners to add the blocks according to them

# Constraints, Assumptions and Dependencies

Constraints:

* Migrating to another blockchain would be a tedious task.
* Cannot interact with web2 based applications.
* Blocks once added cannot be removed.

Assumptions:

* The college admin adding the blocks would maintain its integrity.
* Trusting the blockchain manager and the college to provide authentic certificates.

# High Level System Design

1. Conceptual or logical – This elaborates the logical functional elements of the system. [UML – component or package diagram]
2. Process - Runtime view of the system. [UML – Interaction diagram].
3. Physical – Brief the view of the distributed system. [UML – Deployment diagram].
4. Module – Describe the project management and code organization.
5. Security – Describe the security features of the system.

The Project specifies its purpose into immutable digital certificates, and it can preserve the originality of the certificates and help the students to attain a better solution towards the new technology called blockchain.

Students are also at comparatively low risk of losing the certificate. By using an additional hashing algorithm, we are decreasing the percentage of data being tampered with.

The Hash of the certificate is being stored in the blockchain while the original document will be stored in the Inter Planetary File System (IPFS). This will help us preserve the data and create transparency.

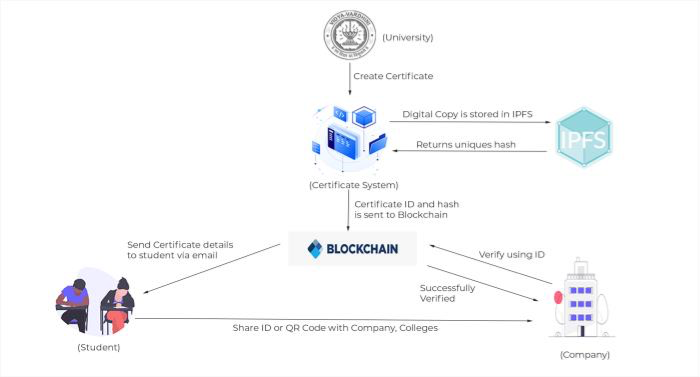
****

Fig. 4.1- High level Design

# Design Description

* 1. **Master Class Diagram**

Diagram

Description automatically generated

Fig. 5.1- Master Class Diagram

* 1. **Reusability Considerations**

Components that can be reused are the smart contracts for the retrieval of documents, proof of authority algorithm, front end design, and backend code for rendering the pages and connecting with blockchain.

* 1. **Use Case Diagram**

Diagram

Description automatically generated

Fig 5.2- Use Case Diagram

1. **ER Diagram / Swimlane Diagram / State Diagram**

**Diagram, schematic

Description automatically generated**

Fig. 6.1- State Diagram

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Entity** | **Name** | **Definition** | **Type** |
| **ENTITIES** | | | | |
|  | Uploader | Faculty | The faculty uploads the document to be added. | Strong |
|  | Viewer | Recruiter | The recruiters can view and verify the student details and documents. | Strong |
|  | Viewer | Student | The students can view and download their documents. | Strong |

Table 6.1- Entity Relation Table

1. **User Interface**

We are going to build a website which will have a login page for the faculty, students and recruiters to login and gain authority to view and download the certificates. The dashboard will consist of the student details and different types of certificates which are owned by the student.

1. **External Interfaces**

**8.1. Hardware Requirements**

* CPU – Must have at least 4.1 Ghz of clock speed.
* RAM – Minimum 8 GB
* Storage – Minimum 10 GB free

**8.2. Software Requirements**

**Operating System:** Any Linux based Operating System (GUI Versions)

**Tools/Libraries:** Remix, Solidity, Web3, IPFS

1. **Design Details**

Novelty – Certificates are being manually verified but in our website the former can verify or authenticate certificates via hashing the content into a cryptographic mode. If the documents are altered, the whole chain disrupts.

Interoperability – The system should perform well on all platforms Related to Web3 Application.

Performance – The performance of the software could Slightly vary as Solidity is comparatively new.

Security – The system should ensure zero vulnerabilities which should ensure the system will not crash and must be able to detect and sustain security attacks.

Reliability - The system should at all times cater the prescribed functionalities and should not deviate from the results/outputs which are expected.

Maintainability-The components/modules included in this project are not very flexible to future changes/modifications.

Portability – Our website is based on web3 and can be accessed through multiple platforms.

Legacy to modernization -The system is open to future modifications and can also be extended to other Web3 Applications. We are following Peer to Peer Architecture rather than client server architecture, where the data is in User’s control.

Reusability- Some components of the proposed system like smart contract blocks can be reused.

Application compatibility-The system will perform well irrespective of the Browser. It is compatible with Metamask wallet and can be accessed using any browser.

# Appendix A: Definitions, Acronyms and Abbreviations

Smart Contract - programs stored on a blockchain that run when predetermined conditions are met. They typically are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary’s involvement or time loss.

IPFS - Interplanetary File System is a protocol and peer-to-peer network for storing and sharing data in a distributed file system.

Blockchain: Blockchain can better be understood as an immutable database and laid the foundation of the whole project. It provides a trusted environment where actions have done are visible and can’t be tampered with.

Metamask: MetaMask is an extension for accessing Ethereum enabled distributed applications or Dapps in your browser. The extension injects the Ethereum web3 API into every website’s JavaScript context so that Dapps can read from the blockchain

# Appendix B: References

1 S. Rajput, A. Singh, S. Khurana, T. Bansal and S. Shreshtha, "Blockchain Technology and Cryptocurrencies," 2019 Amity International Conference on Artificial Intelligence (AICAI), 2019

2 Olnes, S. (2016). Beyond Bitcoin Enabling Smart Government Using Blockchain Technology. In:, et al. Electronic Government. EGOV 2016. Lecture Notes in Computer Science (), vol 9820. Springer, Cham.

3 Abbas, A.A. Cloud-based framework for issuing and verifying academic certificates. Int. J. Adv. Trends Comput. Sci. Eng. 2019, 8, 2743–2749.

4 Wibowo, P.P.A.; Luthfi, M. An Authentic and Secure Printed Document from Forgery Attack by Combining Perceptual Hash and Optical Character Recognition. In Proceedings of the 2019 (ICIMCIS), Jakarta, Indonesia, 24–25 October 2019; pp. 157–162. 4

5 Imam, I. T., Arafat, Y., Alam, K. S., & Shahriyar, S. A. (2021). DOC-BLOCK: A Blockchain Based Authentication System for Digital Documents. 2021 Third (ICICV).

Rama Reddy, T., Prasad Reddy, P.V.G.D., Srinivas, R. et al. Proposing a reliable method of securing and verifying the credentials of graduates through blockchain. EURASIP J. on Info. Security 2021, 7 (2021).

K. Gilani, E. Bertin, J. Hatin and N. Crespi, ”A Survey on Blockchain based Identity Management and Decentralized Privacy for Personal Data,” 2020 2nd Conference on Blockchain Research and Applications for Innovative Networks and Services (BRAINS), Paris, France, 2020

# Appendix C: Record of Change History

[This section describes the details of changes that have resulted in the current High-Level Design document.]

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Date** | **Document Version No.** | **Change Description** | **Reason for Change** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Appendix D: Traceability Matrix

|  |  |
| --- | --- |
| **Project Requirement Specification Reference Section No. and Name.** | **DESIGN / HLD Reference Section No. and Name.** |
| 3.1 Product Features | 5.1 Master Class Diagram |
| 4 Functional Requirement | 9 Packaging and Deployment Diagram |