



PROJECT REPORT

Blockchain (Web3)  
  
 Authentication System

|  |  |  |  |
| --- | --- | --- | --- |
| **Created By:** | Nattuva Sree Swetha | **Approved By:** | <Harshada Topale> |
| **Created On:** | 27-09-2023 | **Approved On:** | DD-MMM-YYYY |

Page left blank intentionally

**INDEX**

[**1** **PROJECT DETAILS** 2](#_Toc143445375)

[**2** **SUMMARY** 2](#_Toc143445376)

[**3** **INTRODUCTION** 2](#_Toc143445377)

[3.1 Background 2](#_Toc143445378)

[3.2 Stakeholders 2](#_Toc143445379)

[3.3 Objectives 2](#_Toc143445380)

[**4** **METHODOLOGY** 3](#_Toc143445381)

[4.1 Considerations & Assumption 3](#_Toc143445382)

[4.2 Approach 3](#_Toc143445383)

[4.3 Activities 3](#_Toc143445384)

[**5** **TARGETTED V/S ACHIEVED OUTPUT** 4](#_Toc143445385)

[**6** **CONCLUSION** 4](#_Toc143445386)

[**7** **APPENDICES** 6](#_Toc143445387)

[7.1 Appendix A – Title 6](#_Toc143445388)

**General Instructions for using the Live Project Report Template**

* This template and the subsequent document created using this template is a confidential document and is the intellectual property of Cloud Counselage Pvt. Ltd. Circulating it outside of the organisation without the consent of Cloud Counselage Pvt. Ltd. is the breach of company policies and will lead to legal actions
* This template is a guideline document to communicate the implementation of design ideas and the results of the work to the stakeholders.
* The **text between inequality (< >) is to be replaced** by relevant text
* Please **remove the yellow highlight on the Text** between the inequality (< >). This is done to help you notice the text to be changed/replaced
* The text in *italics* highlighted in grey is just for reference and should be removed after adding the relevant text

# **PROJECT DETAILS**

|  |  |  |  |
| --- | --- | --- | --- |
| **Project Name** | Authentication System | | |
| **Project Sponsor** | Harshada Topale | | |
| **Project Manager** | Harshada Topale | | |
| **Start Date** | 01-08-2023 | **Completion Date** | 27-09-2023 |

# **SUMMARY**

The project named ‘Authentication System’ was expected to deliver a blockchain based user authentication system to facilitate seamless user identification on a web service. This project was need in order to eliminate the increasing risk of using same credentials (Username – Password) everywhere or linking single account with every service. This Authentication system keeps our employee credentials risk free and authentic. The project involves creating a decentralized authentication system on the Ethereum blockchain. Users register and log in using a Decentralized Identifier (DID) and hashed password. The system integrates a Solidity smart contract for on-chain authentication, while the React.js frontend connects to the blockchain using ethers.js. Key features include off-chain password hashing, event logging, and a structured development lifecycle, addressing security and user experience considerations.

# **INTRODUCTION**

## Background

Over the years, there have been various ways to provide user identity authentication, the most popular and widespread one being a username-password combination. The internet is like an alternate, virtual world that we parallelly dwell in; and just like the physical world, user Identity is a crucial aspect of one's online presence. But using the Same credentials everywhere is not safe and might lead to data breaches and leak of confidential information.

## Stakeholders

* Key Stakeholders: Harshada Topale
* Process Owner: Harshada Topale
* End Customers: Harshada Topale

## Objectives

Creating a blockchain based authentication system for secured user credentials storage and seamless user identification. Through this Authentication system, the user credentials and information are secured by storing them on Ethereum blockchain.

# **METHODOLOGY**

These conventions are all about the positions of line breaks, how many characters should go on a line, and everything in between.

## Considerations & Assumption

Must utilize Ethereum as the primary blockchain platform, front-end should be functional and user-friendly, making username and password redundant. The login shall work through a browser capable of handling cryptographic processes which would be used to sign in the user to authenticator

network.

## Approach

* User requirements
* Designing the Smart Contract
* Code Implementation
* Testing the Smart Contract
* Security Audits
* Deployment to Sepolia Testnet
* Integration with Frontend
* Handling Authentication
* Error Handling
* Iterative Development
* Documentation

## Activities

* Requirement gathering
* Planning
* Designing
* Technology Selection
* Coding
* Testing
* Security Auditing
* Deployment to Sepolia Testnet
* Documentation
* Maintenance

# **TARGETTED V/S ACHIEVED OUTPUT**

In the project plan, the targeted output included the development of a Solidity smart contract for decentralized authentication, frontend integration using ethers.js, off-chain password hashing, event logging, and a smooth user registration/login flow. Achievements aligned with these targets, demonstrating successful implementation. Deviations from the plan, such as deferring user profile management, multi-factor authentication (MFA), cross-blockchain compatibility, governance mechanisms, and integration with emerging Decentralized Identifier (DID) standards, were strategic decisions to manage scope and timelines effectively. The lessons learned involve prioritizing core features, mitigating scope creep, and making informed trade-offs for efficient project delivery. These insights will guide future projects by emphasizing a phased approach and balancing core functionality with potential enhancements. The deviations were strategic decisions made to balance project scope, complexity, and timelines. Lessons learned include the importance of prioritizing core features, managing scope creep, and making informed trade-offs to meet project objectives efficiently. Future projects can benefit from a phased approach, considering both core functionality and potential enhancements.

# **CONCLUSION**

* **Usefulness for Stakeholders**:

**Enhanced Security:** Stakeholders benefit from enhanced security as the system incorporates off-chain password hashing, minimizing the risk of password exposure during registration.

**Transparent Authentication:** The use of Ethereum's decentralized ledger ensures transparency in user registration and login activities. Stakeholders, including users, can verify and audit these actions.

**User Privacy:** Users enjoy increased privacy as the system leverages decentralized identifiers (DID), reducing reliance on centralized identity providers and safeguarding user data.

**Decentralized Nature:** The decentralized authentication system aligns with the principles of blockchain technology, eliminating the need for a central authority. This decentralization benefits stakeholders by removing a single point of failure.

**Efficient User Onboarding:** Stakeholders experience efficient user onboarding facilitated by the smart contract. The process is automated, reducing manual intervention and paperwork traditionally associated with user registration.

* **Future Scope:**

**Integration with DID Standards:** Future enhancements could involve the integration of emerging Decentralized Identifier (DID) standards, such as those proposed by the Decentralized Identity Foundation (DIF). This would align the system with evolving industry standards.

**Smart Contract Upgrades:** The smart contract can be designed to support upgradability, allowing for future improvements and feature additions without requiring a redeployment of the entire contract.

**Cross-Blockchain Compatibility:** Consideration could be given to cross-blockchain compatibility, allowing users to authenticate across different blockchain networks seamlessly.

**User Profile Management:** Future iterations might include user profile management features, enabling users to update their information or link additional attributes to their decentralized identity.

**Governance Mechanisms:** Introduction of governance mechanisms could empower users and other stakeholders to participate in decision-making processes related to the decentralized authentication system.

**Integration with Identity Ecosystem:** Integration with a broader identity ecosystem, including interoperability with existing identity solutions, could be explored to create a more interconnected and versatile authentication framework.

Overall, the decentralized authentication system lays the foundation for a secure and user-centric approach to digital identity, with ample opportunities for future expansion and refinement.

# **APPENDICES**

## Appendix A – Title

Reference - [https://www.dock.io/post/decentralized-identifiers - decentralized-identifiers-and-blockchain](https://www.dock.io/post/decentralized-identifiers#decentralized-identifiers-and-blockchain)