REQUIREMENTS OF THE PROJECT

BLOCKCHAIN-

A blockchain is a distributed ledger with growing lists of records (blocks) that are securely linked together via cryptographic hashes.

ETHEREUM –

Ethereum is a decentralized blockchain with smart contract functionality.

WEB DEVELOPMENT-

Web development is the work involved in developing a website for the Internet (World Wide Web) or an intranet (a private network).

BACKLOGS-

1. User Interface (UI) Enhancements:
    - Improve the user interface design for a more intuitive and user-friendly experience.
    - Address feedback from user testing regarding navigation, layout, and visual aesthetics.
    - Ensure responsive design to optimize usability across different devices and screen sizes.
2. Performance Optimization:
    - Identify and address any performance bottlenecks, such as slow loading times or delays in document processing.
    - Optimize database queries, network communication, and overall system response times.

- Conduct load testing to ensure the platform can handle increasing user demand and transaction volumes.

3. Security Audits and Vulnerability Fixes:
    - Perform regular security audits to identify and address any vulnerabilities or weaknesses in the platform.
    - Address issues identified through penetration testing, code reviews, and vulnerability scanning.
    - Keep up-to-date with the latest security practices and patches to maintain a robust security posture.
4. Compliance with Data Privacy Regulations:
    - Ensure ongoing compliance with relevant data privacy regulations, such as GDPR or local privacy laws.
    - Review and update data handling practices, consent management, and user privacy settings as required.
    - Monitor changes in regulations and adapt the platform accordingly to remain compliant.
5. Integration with Third-Party Services:
    - Integrate with additional identity verification services or document issuers to expand the platform's capabilities.
    - Address any compatibility issues or challenges in integrating with external APIs or systems.
    - Maintain strong partnerships and ensure smooth communication with third-party providers.
6. User Feedback and Iterative Improvements:
    - Continuously gather user feedback and iterate on the platform based on user needs and preferences.
    - Prioritize feature enhancements or bug fixes based on user feedback and business priorities.
    - Implement an iterative development process to regularly release updates and improvements.
7. Scalability and Load Balancing:
    - Address scalability challenges as the user base grows and the number of transactions increases.
    - Implement scaling mechanisms such as sharding, load balancing, or horizontal scaling to handle increased traffic.
    - Monitor system performance and capacity to ensure optimal resource allocation.
8. Cross-Platform Compatibility:
    - Ensure compatibility with different web browsers, operating systems, and mobile devices.
    - Test the platform on various platforms and resolve any compatibility issues that arise.
    - Consider developing native mobile applications for a more seamless user experience on mobile devices.
9. Continuous Monitoring and Incident Response:

- Implement a system for real-time monitoring of the platform's performance, security, and availability.
- Establish an incident response plan to promptly address any system disruptions, security incidents, or data breaches.
- Regularly update and patch system components to address emerging threats and vulnerabilities.

WORKFLOW-

1. User initiates identity verification process.
2. User provides personal information and supporting documents to the identity verification service.
3. Identity verification service validates the provided information and conducts necessary checks (e.g., document verification, background checks).
4. Verified information is hashed and encrypted.
5. Verified identity data is stored on the blockchain.
6. User receives a unique identifier or digital token as proof of verification.
7. User can selectively share their verified identity with trusted parties or service providers.
8. Trusted party requests access to the user's verified identity.
9. User grants permission to share their identity data.
10. Trusted party accesses the blockchain and verifies the authenticity of the shared identity using cryptographic techniques.
11. Trusted party performs additional checks or processes based on the verified identity.
12. Transaction or interaction between the user and trusted party is completed.