Identity Management System Using Block-chain

2303A51L66 - K. VINAY
2303A51L82 - CH. SHASHIVADHAN
2303a51lB7 - J. MOHITH SA

1. *Table of Contents*

1. Overview:

The identity management system will leverage block-chain technology to create a decentralized network where users can create and manage their digital identities securely. Smart contracts will facilitate identity verification, access control, and interactions between users and the block-chain network.

2. Overall Description:

The identity management system will provide users with the ability to create a unique digital identity on the block-chain, which can be verified and used to access various services securely. Users will have control over their identity information and can selectively share it with trusted parties as needed.
The system will consist of a block-chain network where identity-related transactions are recorded as immutable blocks. Smart contracts will govern identity creation, authentication, and authorization processes. Users will interact with the system through a web-based interface, allowing them to manage their identity information and control access to it.

3. Introduction:

In the digital age, managing identities securely and efficiently is paramount. Traditional centralized identity systems pose risks such as data breaches and identity theft. Block-chain technology offers a decentralized and tamper-resistant solution to these challenges by providing a transparent and immutable ledger for identity management.

4. Purpose:

The primary purpose of the project is to develop an identity management system leveraging block-chain technology to address the shortcomings of traditional centralized systems. This includes enhancing security, privacy, and user control over their identities while reducing the risk of identity fraud and unauthorized access.The purpose of this project is to create a secure and decentralized platform for managing identity information, providing users with greater control over their personal data while ensuring transparency and trust through block-chain technology.

5. Scope:

The scope of the project encompasses the design, development, and implementation of a block-chain-based identity management system. It includes features such as user registration, identity verification, access control, and auditability. The system will initially target individual users but could potentially scale to support organizational identities as well.The project will focus on designing and implementing a decentralized identity management system using block-chain. It will include features such as identity creation, authentication, authorization, and selective disclosure of identity attributes. The system will provide a user-friendly interface for managing identity information securely.

6. Technologies to be Used:

Block-chain Platforms: Ethereum or Hyper-ledger Fabric for their mature smart contract capabilities and robust consensus mechanisms.
Programming Languages: Solidity for smart contract development, JavaScript for front-end development, and possibly Python for back-end services.
Cryptographic Protocols: Digital signatures for identity verification, hash functions for data integrity, and possibly zero-knowledge proofs for privacy-enhancing features.
Smart contracts for identity management
Web development technologies for the user interface
Database technologies for storing off-chain data

7. Tools to be Used:

Development Tools: Remix IDE for smart contract development, Truffle framework for testing and deployment, and Metamask for interacting with the Ethereum block-chain.
Version Control: Git for collaborative development and version control.
Testing Frameworks: Truffle Suite for smart contract testing and integration testing with tools like Mocha and Chai.
Block-chain development frameworks
Continuous integration tools

8. Operational Requirements :

Functional Requirements: User registration, identity verification, access control, audit logging, identity attribute management, and secure communication protocols.
Non-functional Requirements: Scalability to support a large number of users, high availability, data privacy and confidentiality, regulatory compliance (e.g., GDPR), and performance benchmarks for transaction throughput and latency.

8.1 Help Desk Support System

users have a 24x7 access to telephone assistance for questions that are technical in nature, such as, slow or sluggish system response time, incompatible browser features, application errors, system downtime inquiries, account lock-out assistance, etc.

8.2 Application Services and Technical support

Programmers and application developers will have access to source code to address bugs or system enhancements as deemed necessary. Network Administrator and DBA support is also required to maintain a 24x7 system uptime.

8.3 Administration Features

System security and access levels are provided in the online system. There are varying levels of system access and functional authority. Each student's access is limited to his/her own registration records. Only authorized system administrator(s) has access to all student registration records.

8.4 System Interface independent of VRU

The VRU system will remain operational and its functionality will be complementary but independent from the online registration system. At any one time, students may use either the VRU system or the online system only, but not both. The online system will be operational even if the VRU system is offline and vice-versa.

8.5 System hardware fail over and routine back up

Computer operations center will handle system hardware tasks such as data tape back-up, hardware maintenance, fail over, scheduled system patches and maintenance

8.6 Audit Trail

System audit trails are inherent part of all user registrations. Among others, all transaction records will capture what action was taken, when (time-stamp) the transaction occurred and who made the transaction.

9. Product Perspective:

The identity management system will integrate with existing applications and services through API s, allowing seamless authentication and identity verification processes. It will complement other block-chain-based applications by providing a secure and decentralized identity layer.
The identity management system will operate within the broader context of block-chain technology, leveraging its decentralized and immutable nature to ensure secure and transparent management of identity information. It will integrate with existing systems through API s for authentication and data exchange.

10. Software Interface:

The software interface will include user-facing interfaces for identity registration, verification, and management, as well as back-end API s for integrating with third-party applications and services.
The system will provide a user-friendly web interface for interacting with identity-related functionalities. Users will be able to create, update, and share their identity information securely. Additionally, API s will be available for integrating the system with other applications.

11. . Hardware Interface:

Hardware interfaces may include integration with hardware wallets or secure hardware modules for cryptographic key storage and identity authentication.
The identity management system will be accessible through standard hardware devices with internet connectivity, such as computers, smartphones, and tablets. There are no specific hardware requirements beyond the devices capable of accessing web-based applications.

12. System Functions:

Key system functions include user registration, identity verification, access control enforcement, audit logging of identity-related transactions, and cryptographic operations for ensuring data integrity and security.

Identity Creation: Users can create their digital identities on the block-chain.
Authentication: Users can authenticate themselves securely using cryptographic techniques.
Authorization: The system provides mechanisms for controlling access to identity information.
Selective Disclosure: Users can selectively disclose identity attributes to third parties as needed.
Identity Revocation: In case of theft or loss of access, users can revoke their identities securely.

13. User Characteristics:

Users of the system will include individuals seeking to establish and manage their digital identities securely, as well as service providers requiring identity verification and access control mechanisms for their applications.
The system is designed to cater to a broad range of users, including individuals, businesses, and organizations. Users should have basic knowledge of block-chain technology and be comfortable with using web-based applications.

14. Constraints:

Constraints may include regulatory requirements related to data privacy and security, technological limitations of block-chain platforms (e.g., scalability, transaction costs), and interoperability challenges with existing identity systems.
Scalability: Ensuring scalability of the system to accommodate a growing number of users and transactions.
Security: Implementing robust security measures to protect against unauthorized access and data breaches.
Compliance: Adhering to regulatory requirements regarding identity management and data privacy.
Assumptions and Dependencies:
Availability of block-chain infrastructure: Dependency on the availability and reliability of the underlying block-chain network.
User adoption: Assumption that users will adopt and trust the decentralized identity management system. Compliance with regulations: Assumption that the system will comply with relevant regulatory frameworks governing identity management and data privacy

15. Assumptions and Dependencies:

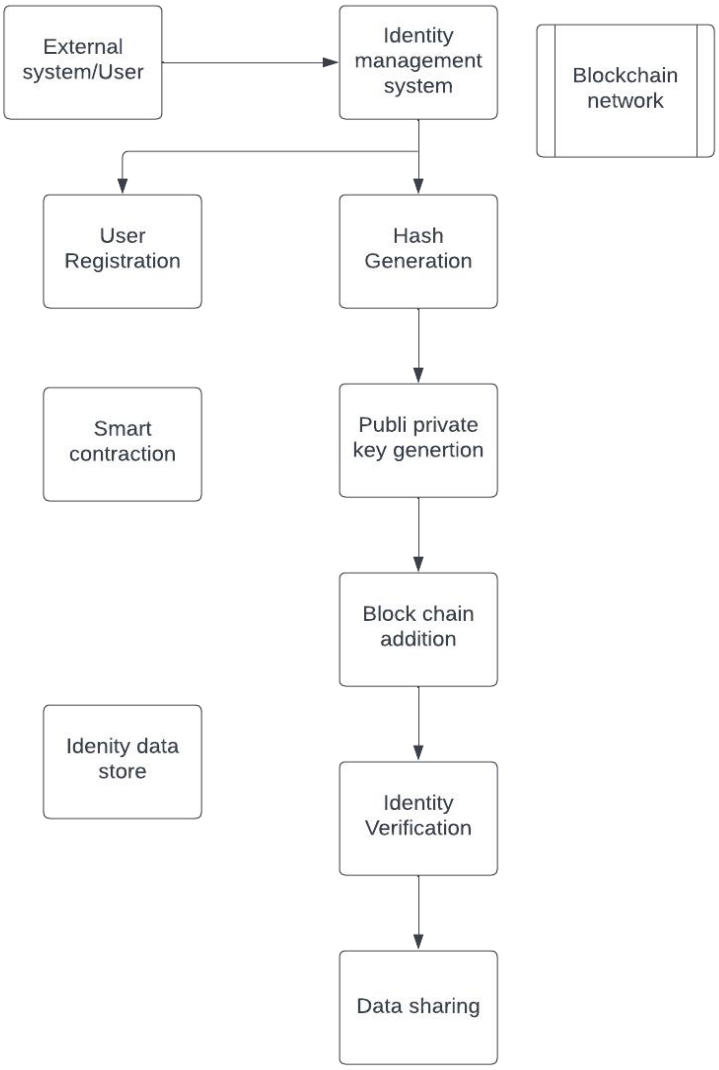
Assumptions may include assumptions about user behavior and adoption, the availability of reliable network infrastructure for block-chain transactions, and dependencies on external services or data sources for identity verification and authentication.
By considering these aspects deeply and thoroughly, you can ensure a comprehensive and effective approach to developing your identity management system using block-chain technology.
Designing an Identity Management System using Block-chain technology is a fascinating project choice, combining principles of software engineering with the decentralized and immutable nature of block-chain. Here's a brief overview of the project along with a suggested prototype to guide you:

16. Project Overview:

Description: The project aims to develop a decentralized identity management system leveraging block-chain technology. Traditional identity management systems often suffer from issues like data breaches, lack of user control over personal information, and centralized points of failure. By utilizing block-chain, the system ensures data integrity, immutability, and user ownership over their identity information.

17. Key Features:

Decentralized Identity Creation: Users can create their digital identities on the block-chain.
Immutable Record Keeping: Identity-related transactions and updates are recorded on the block-chain, ensuring tamper-proof records.
User Control: Users have full control over their identity data and can selectively share it with trusted parties.
Authentication and Authorization: The system provides mechanisms for authentication and authorization using cryptographic techniques.
Privacy Protection: Utilize techniques such as zero-knowledge proofs or selective disclosure to protect user privacy.
Revocation Mechanism: Implement a mechanism for identity revocation in case of theft or loss of access.



Data flow chart

18. Prototype Overview:

Components:

Block-chain Network: Utilize a block-chain platform such as Ethereum or Hyper-ledger Fabric to create a decentralized ledger for identity-related transactions.

Smart Contracts: Develop smart contracts to manage identity creation, updates, and access control rules.

User Interface: Build a user-friendly interface for identity creation, management, and interaction with the block-chain.

Encryption and Key Management: Implement cryptographic algorithms for secure data storage and key management.

Authentication Module: Develop modules for user authentication and authorization, integrating with the block-chain for identity verification.

Revocation Mechanism: Design and implement a mechanism for identity revocation, ensuring the security of the system in case of compromised identities.

Workflow:

Identity Creation: Users initiate the identity creation process by providing necessary information. The system generates a unique identifier and records it on the block-chain.

Identity Verification: Other parties can verify the authenticity of the user's identity by querying the block-chain and verifying the associated transactions.

Identity Updates: Users can update their identity information, and these updates are recorded as transactions on the block-chain.

Selective Disclosure: Users can selectively disclose identity attributes to third parties, maintaining privacy while sharing necessary information.

Revocation: In case of identity theft or loss of access, users can trigger the revocation mechanism to invalidate their identity on the block-chain.

19. Prototype Design:

User Interface: Design a simple, intuitive interface for users to interact with the system. Include options for identity creation, updates, and access control settings.

Block-chain Integration: Implement smart contracts for identity management on a block-chain platform of your choice. Ensure secure communication between the user interface and the block-chain network.

Authentication Module: Develop modules for user authentication using cryptographic techniques. Integrate with the block-chain for identity verification.

Privacy Enhancements: Implement privacy-enhancing techniques like zero-knowledge proofs or selective disclosure to protect user privacy.

Revocation Mechanism: Design and implement a mechanism for identity revocation, considering security implications and user experience.

20. Conclusion:

The Identity Management System Using Block-chain project offers a unique opportunity to explore the intersection of software engineering and block-chain technology. By following the suggested prototype and incorporating key features, you can develop a robust system that addresses the challenges of traditional identity management while leveraging the benefits of block-chain decentralization and immutability.

21. Process Requirements

The following are among the inherent requirements that the online registration system must be able to handle.

21.1 DB2 transaction

The system must be able to send, receive and trigger transaction to the DB2 registration database system.

21.2 Data integrity

Commit transactions that are completed and/or rollback unfinished or time-out transactions.

21.3 Data validation

Data error from the user's end and from the back-end database-processing end must be gracefully handled. There will be data validation and error-handling routines as part of the online registration system.

21.4 Performance

Must resolve locking issues and handle concurrent use of the system on a 24x7 basis. Send, receive and display user messages to assist the over-all user experience.

21.5 Data repository

The online registration system will maintain the existing DB2 registration database as the main repository of data.

22. Output Requirements

22.1 Transaction summary and confirmation

Each online registration user must have a view of summary of actions done for a particular session or a particular registration function. The DB2 registration database will be able to display all successfully committed transactions.

22.2 Exception reports

System exception reports must be consolidated to record special user records or special conditions not normally handled using regular registration procedures. Examples are conditionally accepted user pending completion of banking transaction, international user pending acceptance of bitcoin score, etc.

22.3 Registration Reports and summaries

Registrar and administrators must be able to extract summarized and rolled-up data into meaningful information. All records will be archived but accessible on demand.

23. Hardware Requirements

23.1 Network

database network infrastructure (wired and wireless)

23.2 Client Computers

Mac, Unix and Windows client computers

23.3 IBM Mainframe

The environment that will host the world-wide databases

23.4 Production support systems

Web server computer(s) and related hardware support (back-up tapes, redundant drives, UPS, etc.)

24. Software Requirements

24.1 Client Operating Systems

UNIX (any flavor) ,MAC , Windows

24.2 Client Application

Java and Java Script compatible browser: Netscape , IE, Opera

24.3 Network system Network

software and protocols in order for systems to communicate: TCP/IP, HTTP, HTTPS,FTP

24.4 Mainframe system

IBM Gateway , DB2 database

24.5 Licenses

Valid licenses are required to run software from third party vendors: To use application development tools, To use web server, application server and database software in development, test and production mode