COMP842_2024_S1_Applied Blockchains and Cryptocurrencies

Decentralized Identity Management System Using Decentralized Identifiers (DIDs) on the Ethereum Blockchain

NAME	STUDENT ID
ROHAN HOLEGADDE SURESH	24227139
VAISHNAV RAJENDRA PRASAD	23202577
PRANAV SUSHIL	23215353

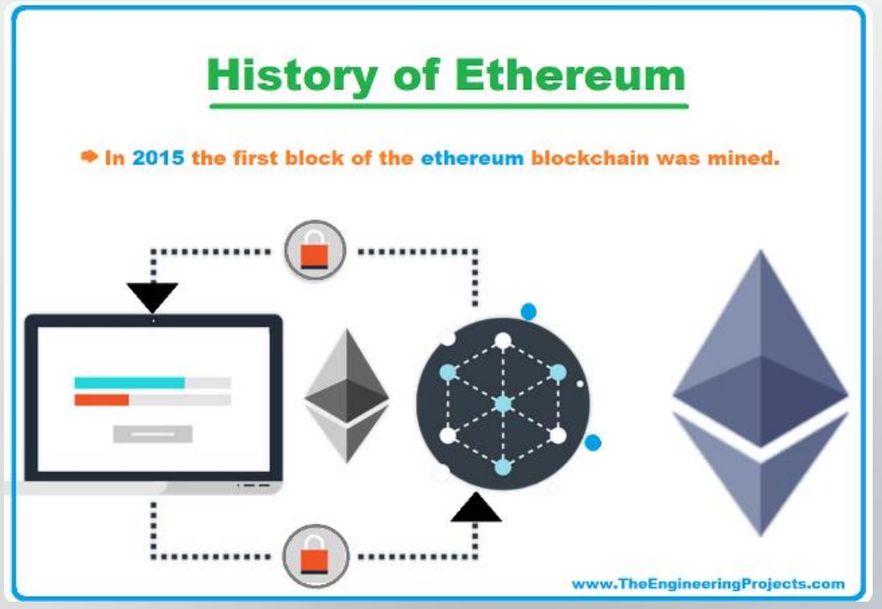
INTRODUCTION

In today's digital age, identity theft has become a growing concern, posing significant risks. As we increasingly rely on blockchain technology for various applications, ensuring the security and integrity of digital identities of individual within these networks is of utmost importance. This project aims to solve this critical issue by developing a decentralized identity system using Decentralized Identifiers (DIDs) on the Ethereum blockchain.

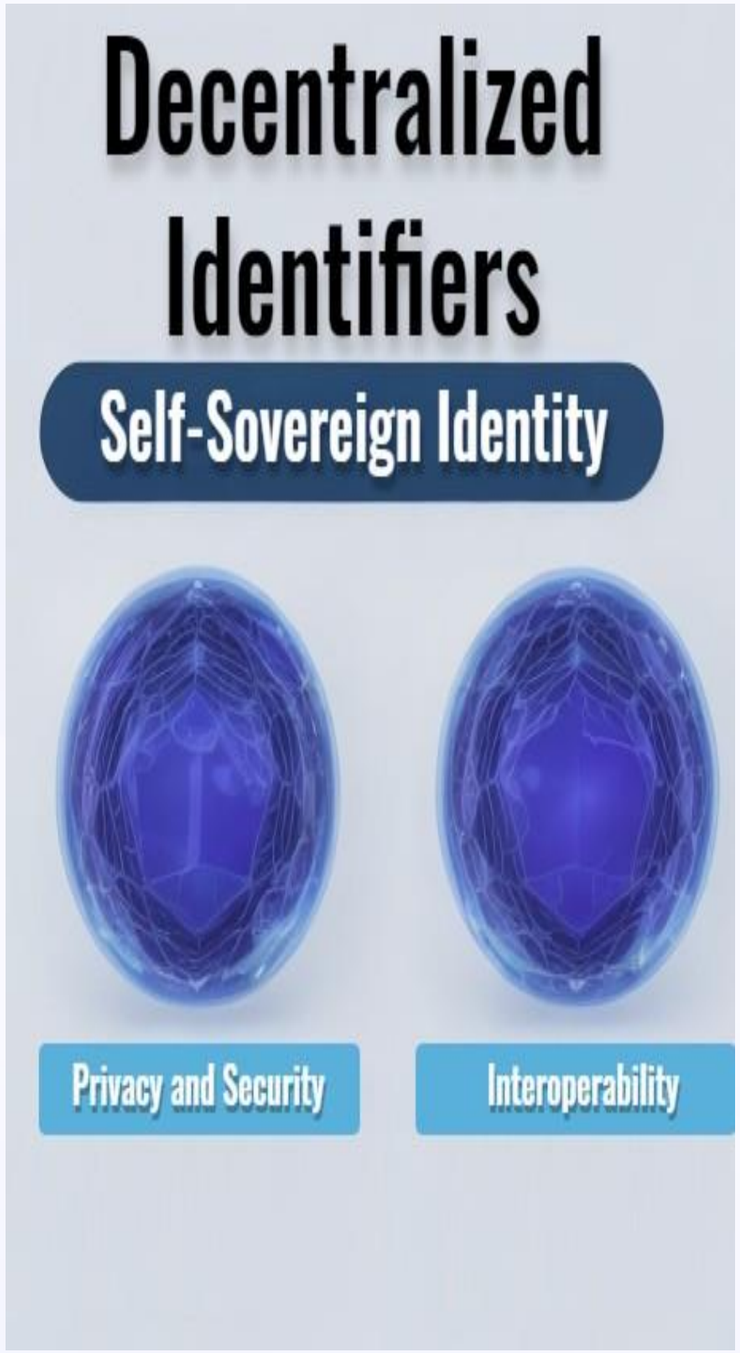
Our proposed solution leverages the power of DIDs and the Ethereum blockchain to create a secure, transparent, and user-centric identity management system. Enable individuals to have full control over their digital identities while preventing identity theft and unauthorized access to personal information.

The significance of this project lies in its potential to revolutionize the way we manage and protect our digital identities. By providing a decentralized and tamper-proof solution, eliminate the need for centralized authorities and empower users to maintain complete control over their personal data. This not only enhances privacy and security but also fosters trust and accountability within blockchain networks.

Ethereum and Decentralized Identity (DIDs)



- Ethereum is a decentralized, open-source blockchain platform that enables the deployment and utilizes PoS. In this system, validators stake their ETH tokens to secure the network. Validators are randomly chosen to validate new blocks and add them to the blockchain ,and execution of smart contracts. It provides a foundation for building decentralized applications (DApps) that can leverage the security, immutability, and transparency of the blockchain.
- In the context of our project, Ethereum serves as the underlying infrastructure for implementing a decentralized identity system using Decentralized Identifiers (DIDs). By integrating DIDs into Ethereum smart contracts, we can create a secure and verifiable way to manage user identities without relying on centralized authorities.
- Ethereum's smart contract functionality allows us to define the rules and logic for creating, updating, and resolving DIDs. The DID registry smart contract acts as a central component, managing the lifecycle of DIDs and their associated metadata. Users can interact with the DID registry contract to create new DIDs, update their information, and prove their identity to other smart contracts.
- The Ethereum blockchain provides a tamper-proof and transparent ledger for storing DID-related transactions and data. This ensures the integrity and immutability of the identity information, making it resistant to unauthorized modifications or attacks.



Understanding DIDs

Unique and Cryptographically Verifiable

DIDs are unique, cryptographically verifiable identifiers that represent an entity, whether a person or organization. They are controlled by the entity itself, not by a central authority, ensuring user autonomy and privacy.

Self-Sovereign Identity

DIDs enable a self-sovereign identity model, where users have full control over their digital identities and can selectively disclose personal information to third parties without relying on a centralized intermediary.

Blockchain Integration

DIDs are often integrated with blockchain platforms, such as Ethereum, to leverage the immutable and decentralized nature of the underlying distributed ledger technology for secure storage and verification of DID documents.

Identity theft attacks in Ethereum

Grinding attack

Attack: tries to cheat the system to get more chances to create new blocks on the blockchain. This increases probability of being selected for block minting. This is unfair and harms the network's security.

Rectification with DIDs:
•DIDs act like unique usernames that are hard to fake. Imagine a special ID card for your account on the blockchain.
•Past behavior on the network is linked to your DID.
•Be good (honest validation) = higher reputation = more rewards.
•Be bad (cheating) = lower reputation = fewer rewards.

Sybill Attacks

Attack: Attackers create multiple fake identities to manipulate voting or reputation systems within Ethereum applications.
Rectification with DIDs:

- •DIDs provide a unique and verifiable identity for each user, making it harder to create multiple fake identities.
- •DIDs can be linked to reputation scores based on past behavior on the network. Validators with higher reputations could have more voting power, making it less beneficial to create fake identities.
- •Smart contracts can implement identity verification mechanisms based on DIDs, ensuring that each user has a single, authenticated identity.
- Reputation systems can be built on top of DIDs, allowing for more accurate and trustworthy assessments of user behavior.

Keystore File Theft

Attack: Attackers gain unauthorized access to a user's keystore file, which contains their private keys, enabling them to steal funds or perform unauthorized transactions.
Rectification with DIDs:

- DIDs allow users to have multiple keys associated with their identity, providing a more flexible and secure key management system.
- Users can rotate or revoke keys associated with their DID without losing their overall identity.
- Smart contracts can verify user identities based on the DID's cryptographic proofs, reducing the reliance on a single keystore file.

Man In middle attack

Attack: Attackers intercept the communication between a user and a smart contract, allowing them to modify or steal sensitive information.

Rectification with DIDs:
•DIDs enable secure communication channels between users and smart contracts using encryption and digital signatures.
•The DID document contains public keys and service endpoints that allow for secure and authenticated communication.
•Smart contracts can verify the integrity and authenticity of the communication based on the DID's cryptographic proofs, preventing unauthorized modifications.

Ethereum Smart Contract Fundamentals

1

Smart Contract Development

Developers write smart contract code using high-level languages like Solidity, vyper defining the contract's functionality, state variables, and functions.

2

Compilation and Deployment

The smart contract code is compiled into bytecode executable by the Ethereum Virtual Machine (EVM), and then deployed to the Ethereum blockchain by sending a transaction.

3

Interaction and Execution

1. Ethereum nodes participate in the blockchain network, validating transactions and maintaining consensus.
2. Smart contracts are deployed to the Ethereum blockchain and assigned unique addresses.
3. Users interact with smart contracts by sending transactions to their addresses.
4. Ethereum nodes process the transactions, execute the smart contract code, and update the contract's state on the blockchain.
5. The updated state is transfered to all nodes in the network, ensuring consistency and immutability.

Integration of Decentralized Identifiers (DIDs)

DID Registry Contract

A DID (Decentralized Identifier) registry is a smart contract deployed on a blockchain network, such as Ethereum, that manages the creation, updating, and resolution of DIDs. It serves as a central directory or database for storing and managing DID-related information.

Identity Verification

Identity Verification: The Identity Verification component focuses on validating and authenticating the identity associated with a DID. It provides mechanisms to verify DID ownership through digital signatures and encryption methods. This ensures that the entity claiming a specific DID is indeed the rightful owner.

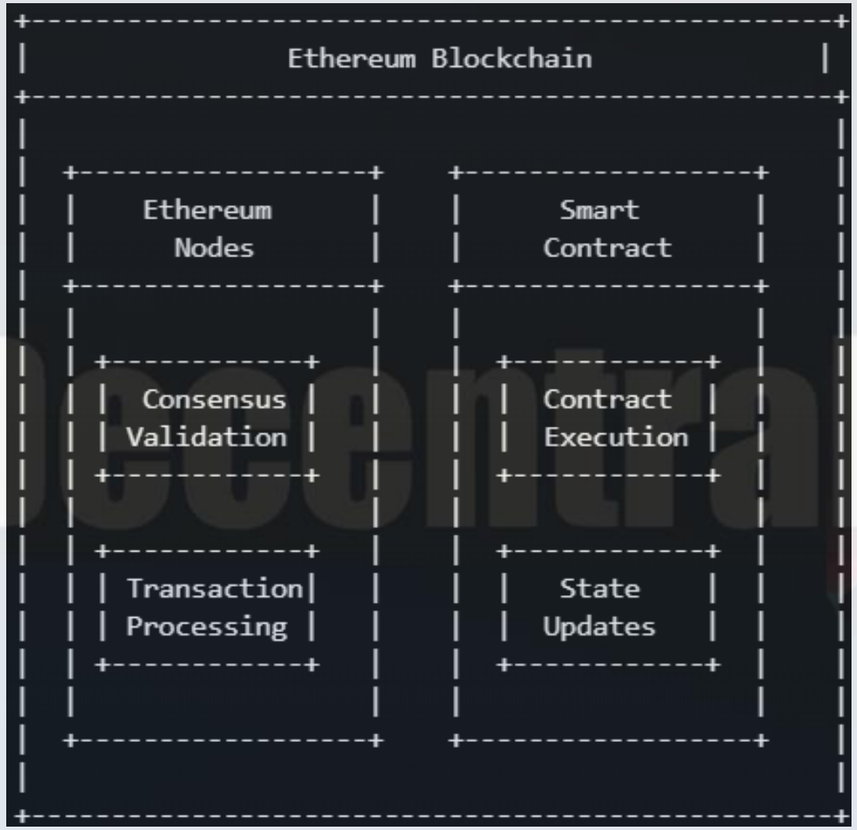
Identity Verification also includes authentication methods such as biometric data and multi-factor authentication to strengthen the identity verification process. Additionally, it supports the verification of claims and attestations associated with a DID, such as issued credentials, to establish trust and credibility.

DID Creation

Smart contracts can Users create new DIDs by interacting with the DID registry contract.

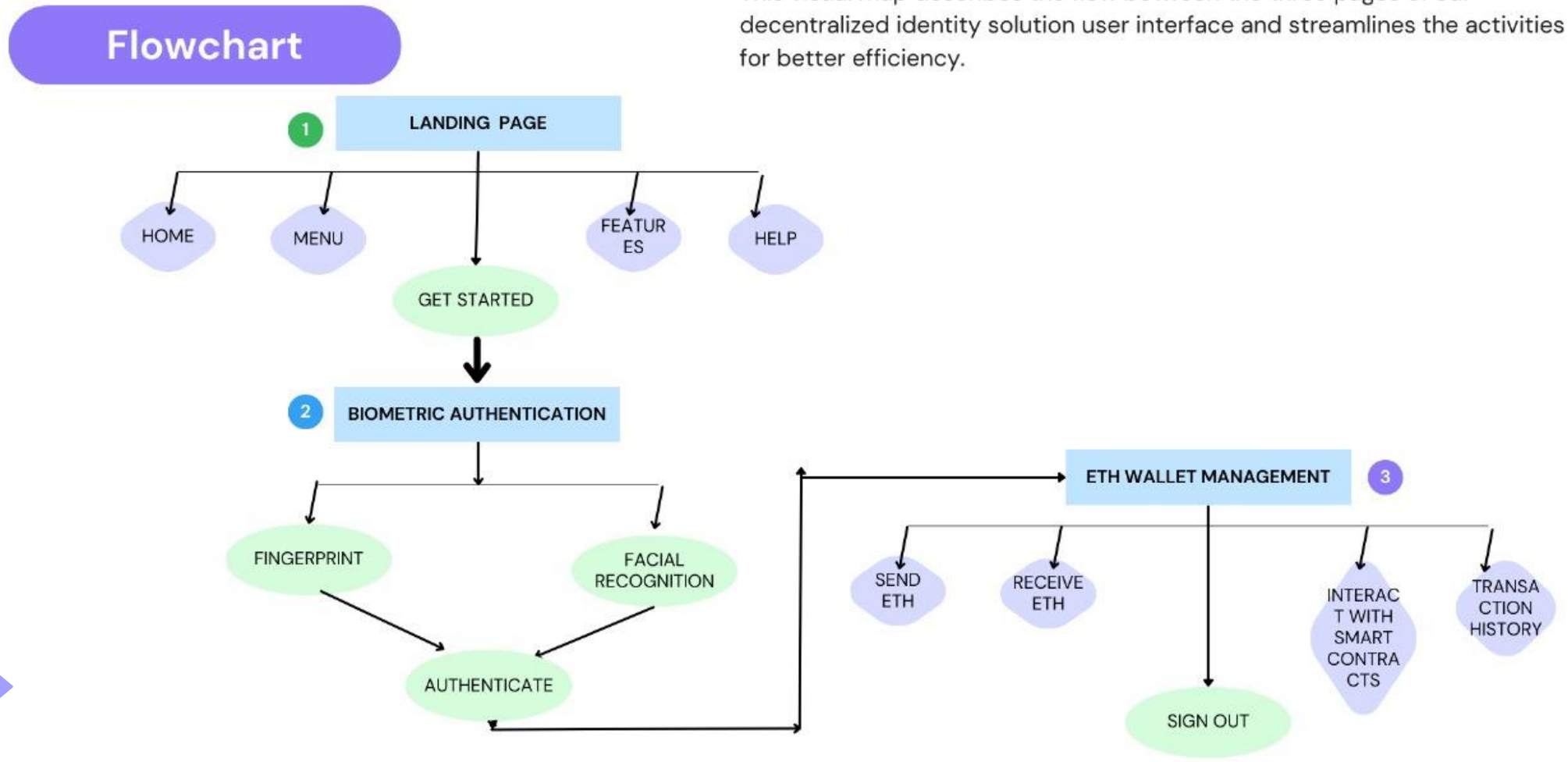
- They provide the necessary information, such as public keys and authentication methods.
- The DID registry contract assigns a unique DID to each user and stores the associated DID document on the blockchain very the DID registry to retrieve the corresponding DID document, which contains metadata associated with the DID, such as public keys and authentication methods.

This workflow represents how blockchain can be used for secure and decentralized identity management and access control in Ethereum.



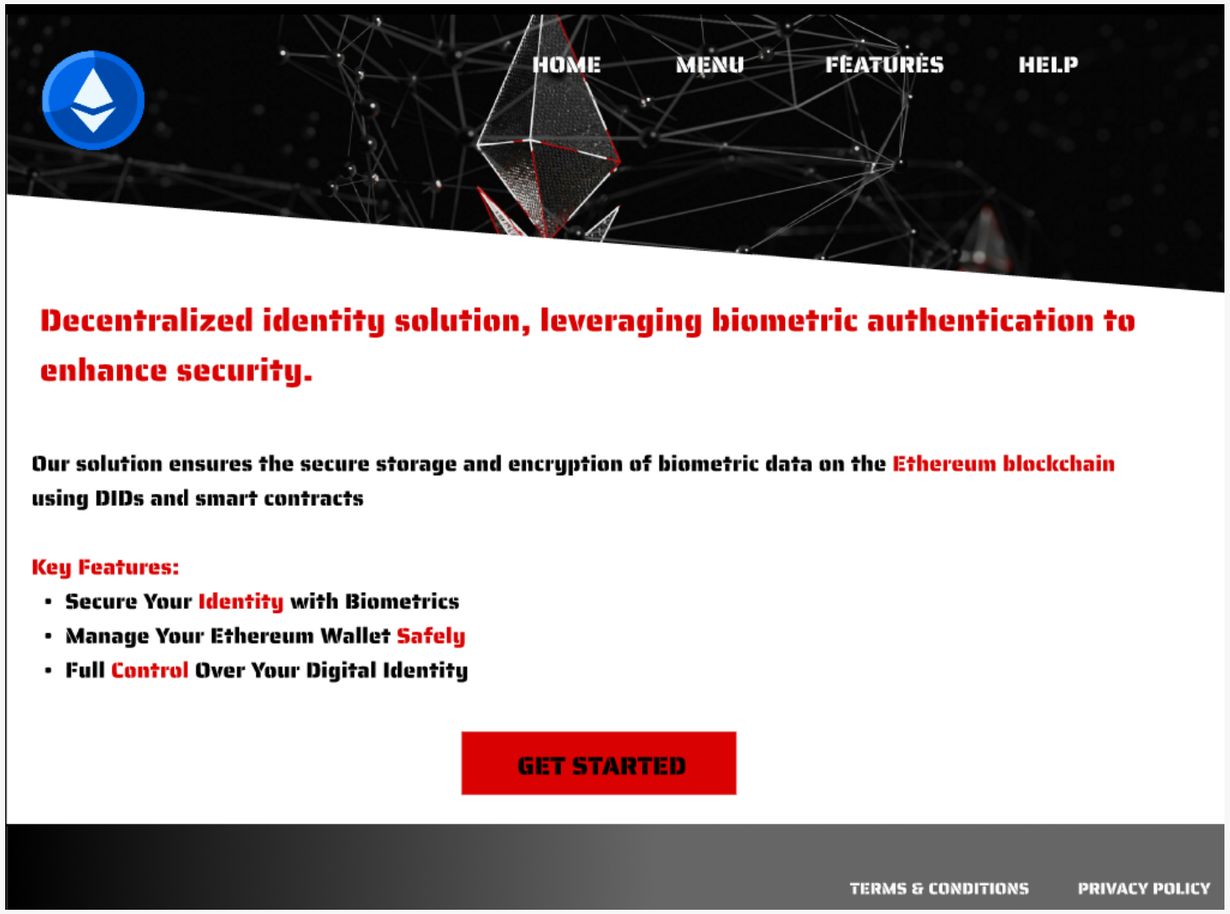
SYSTEM DESIGN

This visual map describes the flow between the three pages of our decentralized identity solution user interface and streamlines the activities for better efficiency.



SYSTEM DESIGN

Page 1

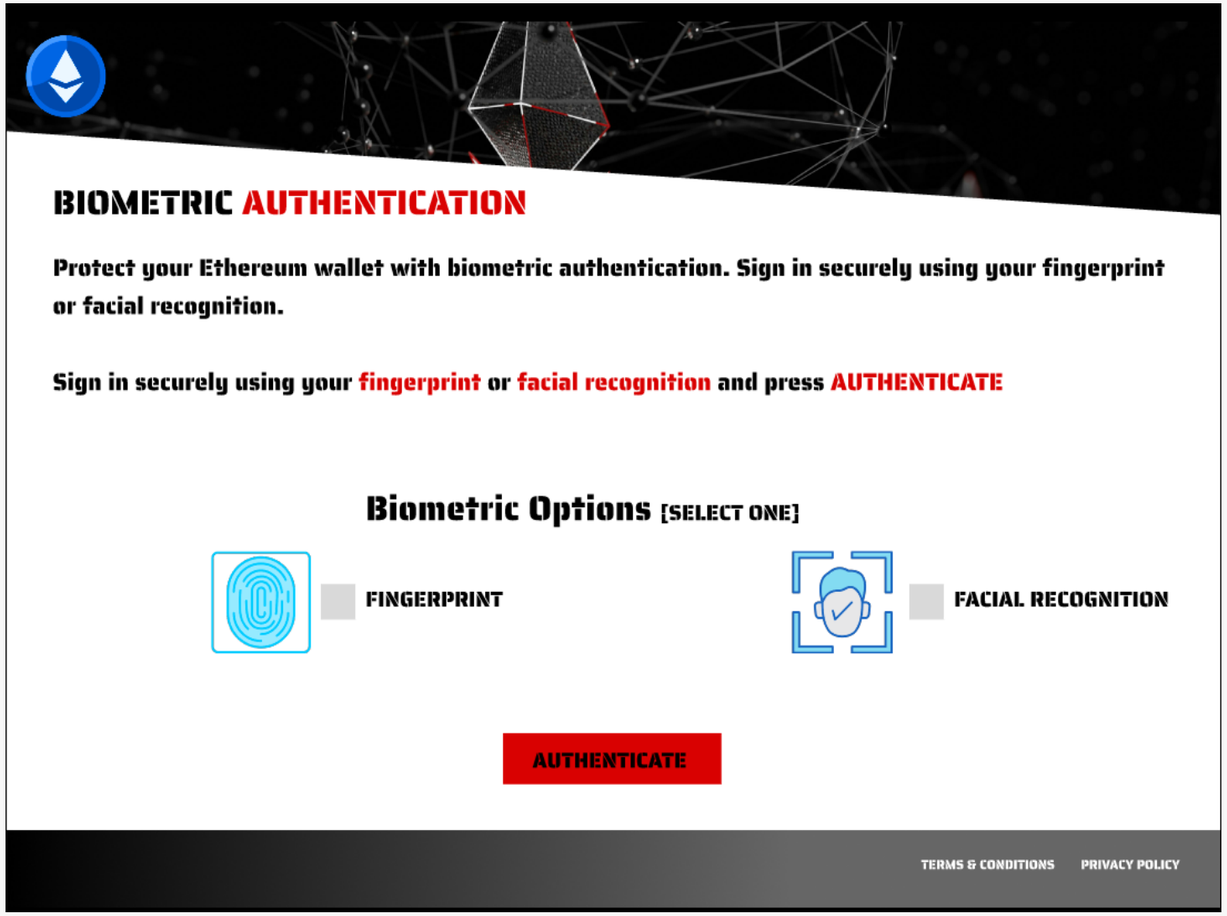


Key Features:

- Secure Your Identity with Biometrics:
  Utilize biometric authentication methods such as fingerprint and facial recognition for enhanced security."
- Manage Your Ethereum Wallet Safely:
  Safely manage your Ethereum wallet with cutting-edge security protocols and user-friendly interfaces."
- Full Control Over Your Digital Identity:
  Empower users with self-sovereign identities, giving them complete control over their digital presence and personal information.

Call to Action: Get started by clicking the 'Get Started' button to begin the secure authentication process.

Page 2 Biometric Authentication Page

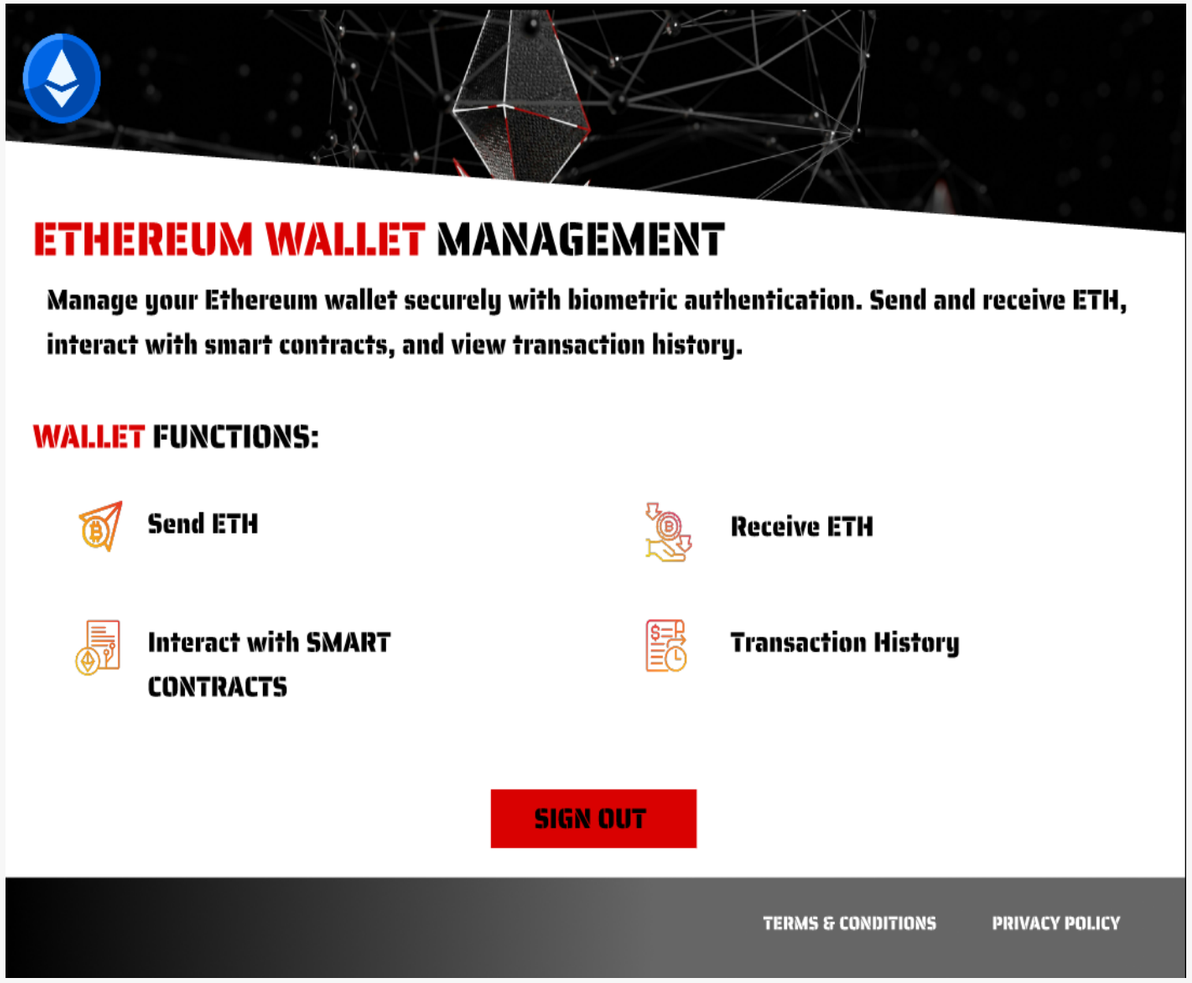


Instructions:

- Select your preferred biometric option:
  - **Fingerprint:** Authenticate using your unique fingerprint pattern for a secure sign-in process.
  - **Facial Recognition:** Authenticate using facial recognition technology, which scans your facial features to verify your identity.

- Once selected, press the 'Authenticate' button to proceed.

Page 3 Ethereum Wallet Management Page



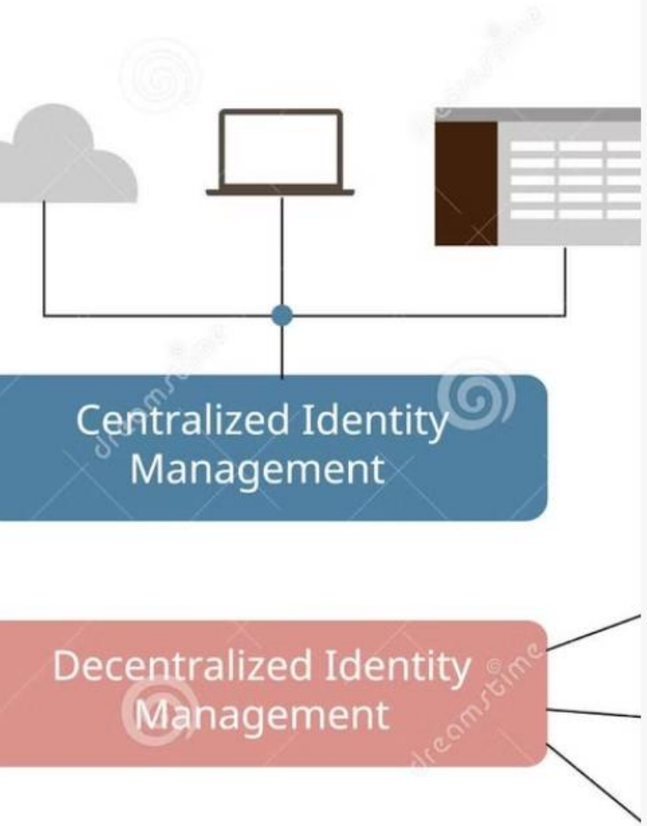
Wallet Functions

- Send ETH: Transfer Ethereum to other users securely and efficiently with a few simple clicks.

- Receive ETH: Receive Ethereum from other users into your wallet. Your biometric authentication ensures the security of incoming transactions.

- Interact with Smart Contracts: Engage with decentralized applications (DApps) and execute smart contracts directly from your wallet. This function opens up a world of possibilities for decentralized finance (DeFi) and other blockchain-based services.

- Transaction History: View and manage your transaction history. Keep track of all your transactions, ensuring transparency and ease of record-keeping.



Access Control and Privacy with DIDs

1

Identity Verification

Once a user's identity is verified using their DID, the smart contract can implement access control mechanisms based on the authenticated DID.

2

Access Control

- The contract can compare the DID with predefined access control lists or permission structures to determine the user's authorization level.

  - Based on the authorization, the smart contract grants or denies access to specific functions or resources

3

Selective Disclosure

DIDs support selective disclosure, allowing users to share only the necessary information required for a specific interaction.

  - Users can provide specific claims or attestations from their DID document, rather than revealing the entire document.

  - This enables privacy-preserving interactions, where users have control over the information they share.

Ecosystem Integration and Interoperability

Ethereum Integration

Ethereum-based DIDs can be recognized and used by other DID-compatible systems, enabling seamless integration and collaboration within the decentralized identity ecosystem.

Interoperability

DIDs provide a standardized way to represent identities across different systems and platforms, allowing for cross-application and cross-platform identity management. For instance , Dapps

EVALUATION

Functionality and Security:

- Test smart contracts for reliability and correct DID management.
- Evaluate security against attacks and privacy safeguards.

Performance and Scalability:

- Measure transaction efficiency and scalability under load.
- Analyze gas usage and explore scaling solutions.

Usability and Integration:

- Ensure user-friendly integration with Ethereum apps.
- Gather feedback on user experience and interface.

Interoperability and Compliance:

- Verify adherence to W3C DID standards and GDPR.
- Test compatibility with other identity systems.

FUTURE SCOPE

1. Enhanced Privacy Mechanisms: Further research and implementation of advanced cryptographic techniques such as homomorphic encryption and multi-party computation to enhance privacy and data protection.
2. Interoperability Improvements: Developing protocols to ensure seamless interoperability between different blockchain networks and identity systems, enabling a more cohesive decentralized identity ecosystem.
3. User Experience Optimization: Conducting extensive user studies to refine the user interface and experience, ensuring the system is accessible and easy to use for non-technical individuals.
4. Real-world Implementation: Piloting the system in real-world scenarios with various stakeholders, including enterprises and government agencies, to gather practical insights and drive widespread adoption.
5. Integration with Emerging Technologies: Investigating the integration of DIDs with emerging technologies such as IoT and AI to expand the applicability and functionality of the decentralized identity system.

CONCLUSION

1. Comprehensive Approach to Identity Management

2. User-Centric Identity Control

3. Blockchain Advantages

4. Secure and Private Identities

5. Thorough Testing and Evaluation

6. Transformative Potential

CONCLUSION

Ethereum Smart Contracts	Decentralized Identifiers (DIDs)
- Self-executing digital agreements on the Ethereum blockchain - Enable a wide range of decentralized applications (dApps) - Require careful consideration of gas consumption and transaction fees	- Provide a standardized way to represent digital identities - Empower users with control over their personal data - Support secure authentication and privacy-preserving interactions - Facilitate interoperability across decentralized identity systems

By integrating Ethereum smart contracts and decentralized identifiers (DIDs), developers can create powerful decentralized applications that prioritize user privacy, security, and control over personal data. This powerful combination unlocks new possibilities for building a more equitable and transparent digital ecosystem.

THANK YOU