WEB 3.0

PROBLEM STATEMENTS

1. Decentralized Digital Identity Management

Problem Statement

Digital identities are currently controlled by centralized platforms, exposing users to privacy risks and identity misuse. A decentralized approach is required to give users full ownership of their digital identity.

Core Challenge

- Design a self-sovereign identity system
- Enable secure issuance and verification of credentials
- Support selective disclosure of identity data
- Ensure interoperability across platforms
- Prevent identity theft and unauthorized use

2. Smart Contract–Based Secure Data Sharing

Problem Statement

Sharing sensitive data across organizations relies on centralized intermediaries, increasing trust and security risks. A decentralized mechanism is required to control data access transparently.

Core Challenge

- Use smart contracts to manage data access rules
- Enforce user consent and permissions automatically
- Ensure auditable and tamper-proof access logs

- Prevent unauthorized data usage
- Minimize reliance on trusted intermediaries

3. Decentralized Storage System with Access Control

Problem Statement

Centralized cloud storage introduces single points of failure and limits user control over data. A decentralized storage system is needed to ensure ownership, availability, and security.

Core Challenge

- Design decentralized storage architecture
- Guarantee data availability and integrity
- Implement cryptographic access control
- Ensure long-term data persistence
- Enable secure and private data retrieval

4. DAO-Based Governance for Organizations

Problem Statement

Traditional governance systems lack transparency and inclusive participation. Decentralized Autonomous Organizations (DAOs) offer a transparent alternative but require robust governance models.

Core Challenge

- Enable transparent proposal creation
- Implement fair and secure voting mechanisms
- Execute decisions via smart contracts

- Prevent governance attacks and manipulation
- Maintain decentralization and scalability

5. Token-Based Incentive Mechanisms in Web 3.0 Platforms

Problem Statement

Decentralized platforms struggle to align user incentives with long-term ecosystem growth. Poorly designed token systems can encourage misuse or short-term gains.

Core Challenge

- Design fair token distribution models
- Incentivize honest participation
- Discourage malicious behavior
- Balance short-term rewards and long-term sustainability
- Align incentives with governance and platform goals

6. Privacy-Preserving Transactions Using Zero-Knowledge Proofs

Problem Statement

Public blockchains expose transaction details, raising serious privacy concerns. Users need transaction privacy without compromising security or decentralization.

Core Challenge

- Integrate zero-knowledge proof mechanisms
- Validate transactions without revealing sensitive data
- Protect identities, amounts, and transaction history

- Maintain scalability and performance
- Ensure compatibility with existing blockchains

7. Cross-Chain Interoperability for Web 3.0 Applications

Problem Statement

Blockchain networks operate in isolation, limiting usability and innovation. Web 3.0 applications require secure interoperability across multiple chains.

Core Challenge

- Enable secure cross-chain communication
- Support asset transfer and message passing
- Verify state across heterogeneous blockchains
- Prevent cross-chain exploits
- Preserve decentralization and trust minimization

8. Decentralized Access Control for Web 3.0 Applications

Problem Statement

Many decentralized applications rely on static roles or centralized access control, limiting flexibility and security. A decentralized access management model is required.

Core Challenge

- Implement smart contract–based access control
- Support dynamic roles and permissions
- Enable access revocation and delegation

- Avoid centralized authority or control points
- Maintain strong security guarantees

9. Secure and Transparent NFT Ownership Management

Problem Statement

NFT ecosystems face issues with ownership verification, metadata tampering, and long-term availability. A reliable ownership management system is required.

Core Challenge

- Ensure verifiable NFT ownership and provenance
- Maintain integrity of NFT metadata
- Use decentralized storage for persistence
- Prevent tampering and unauthorized modification
- Improve transparency and trust in NFT platforms

10. Decentralized Reputation Systems for Web 3.0 Platforms

Problem Statement

Trust between anonymous participants in decentralized ecosystems is difficult to establish. Centralized reputation systems undermine decentralization.

Core Challenge

- Build reputation from verifiable on-chain activity
- Preserve user privacy
- Prevent Sybil and manipulation attacks

- Accurately reflect participant behavior
- Avoid centralized reputation authorities