International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 05 | May - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Web Based Hierarchical Deterministic wallet

1. Naval Kishor Jha
menavaljha@gmail.com
Department of Information Technology

2. Amul Gaurav
amulgaurav907@gmail.com
Department of Information Technology

3.Md Sharik Ahamed
sharikahamed20@gmail.com
Department of Information Technology

4.Ritesh Sharma
riteshsharma1897299@gmail.com
Department of Information Technology

Suman Rani
Assistant Professor
Department of Information Technology

Abstract

- Pixel-Web3 Wallet is a hierarchical deterministic (HD) wallet designed for secure and decentralized asset management across multiple blockchain networks, including Ethereum and Solana. Unlike traditional wallets that depend on browser extensions or centralized servers, Pixel offers a web-based solution with user-controlled security through locally stored seed phrases. This paper explores the wallet's architecture, security framework, and innovative features, such as real-time balance updates and flexible recovery options. Additionally, the research evaluates the scalability of Pixel and its potential expansion to support more blockchain networks. By eliminating reliance on third-party services, Pixel enhances accessibility while maintaining strong security, making it a promising solution for blockchain enthusiasts, traders, and developers.

Keywords: Blockchain, HD Wallet, Cryptocurrency,Web3,Ethereum,Solana, Security

Introduction: Pixel is a secure, hierarchical deterministic (HD) wallet created for managing and transacting with assets across different blockchain networks directly from a web browser. Blockchain technology's decentralized nature and the rise in popularity of cryptocurrencies have emphasized the need for secure and easy-to-use wallet solutions. Pixel fulfills this requirement by offering support for Ethereum and Solana blockchains, allowing users to manage multiple addresses and assets within one wallet. Unlike many wallets that require a browser extension or server dependency, Pixel is entirely web-based, allowing users to access their wallets securely from any browser without additional installations. The wallet's focus on user-controlled seed phrases and secure local storage offers a more private, user-centric experience, with added features such as real-time balance updates and flexible recovery options.

- **Background**: The rapid adoption of blockchain technology has led to an increasing demand for secure, user-friendly cryptocurrency wallets. Many existing solutions, such as MetaMask (Ethereum) and Phantom (Solana), require browser extensions or centralized servers, which introduce security risks and dependency on third-party services. These traditional wallets store private keys or sensitive data in ways that may be vulnerable to phishing attacks, malware, or server breaches.

To address these challenges, **Pixel-Web3 Wallet** provides a decentralized, multi-chain HD (Hierarchical Deterministic) wallet that allows users to manage their blockchain assets securely within a web-based environment. Unlike conventional wallets, Pixel does not rely on browser extensions or centralized storage; instead, it ensures user-controlled security by managing seed phrases locally.

- **Literature Review**:

Existing blockchain wallets primarily fall into two categories:

1. **Browser Extension Wallets** – Popular solutions like **MetaMask** and **Phantom** provide convenient access but require installation, making them susceptible to phishing and security vulnerabilities.

2. **Centralized Web Wallets** – Some wallets rely on third-party servers to manage user accounts, increasing the

risk of data leaks and unauthorized access.

HD wallets have become a preferred choice in cryptocurrency security due to their deterministic key generation mechanism. Research highlights that **HD wallets improve security and usability** by deriving multiple addresses from a single seed phrase, reducing reliance on private key storage. However, most multi-chain wallets still rely on extensions or centralized platforms, leaving a gap for a **web-based, self- custodial** alternative.

- **Objectives**: Develop a secure, multi-chain HD wallet Enable seamless asset management from any web browser

Provide user-controlled security with local seed phrase storage Ensure real-time balance updates without page reloads

- **Significance**: Pixel-Web3 Wallet introduces an innovative approach by integrating multi-chain support with a user-friendly, decentralized web-based interface. By eliminating dependency on centralized services, it enhances both **accessibility and security**, making it an ideal choice for blockchain users, developers, and traders. This project aims to set a new standard for secure, extension-free cryptocurrency wallets while maintaining flexibility for future blockchain integrations.

Methodology (Methods)

- **Research Design**

The development of Pixel-Web3 Wallet follows an applied research approach, integrating frontend, blockchain interaction, and security mechanisms to create a decentralized web-based wallet.

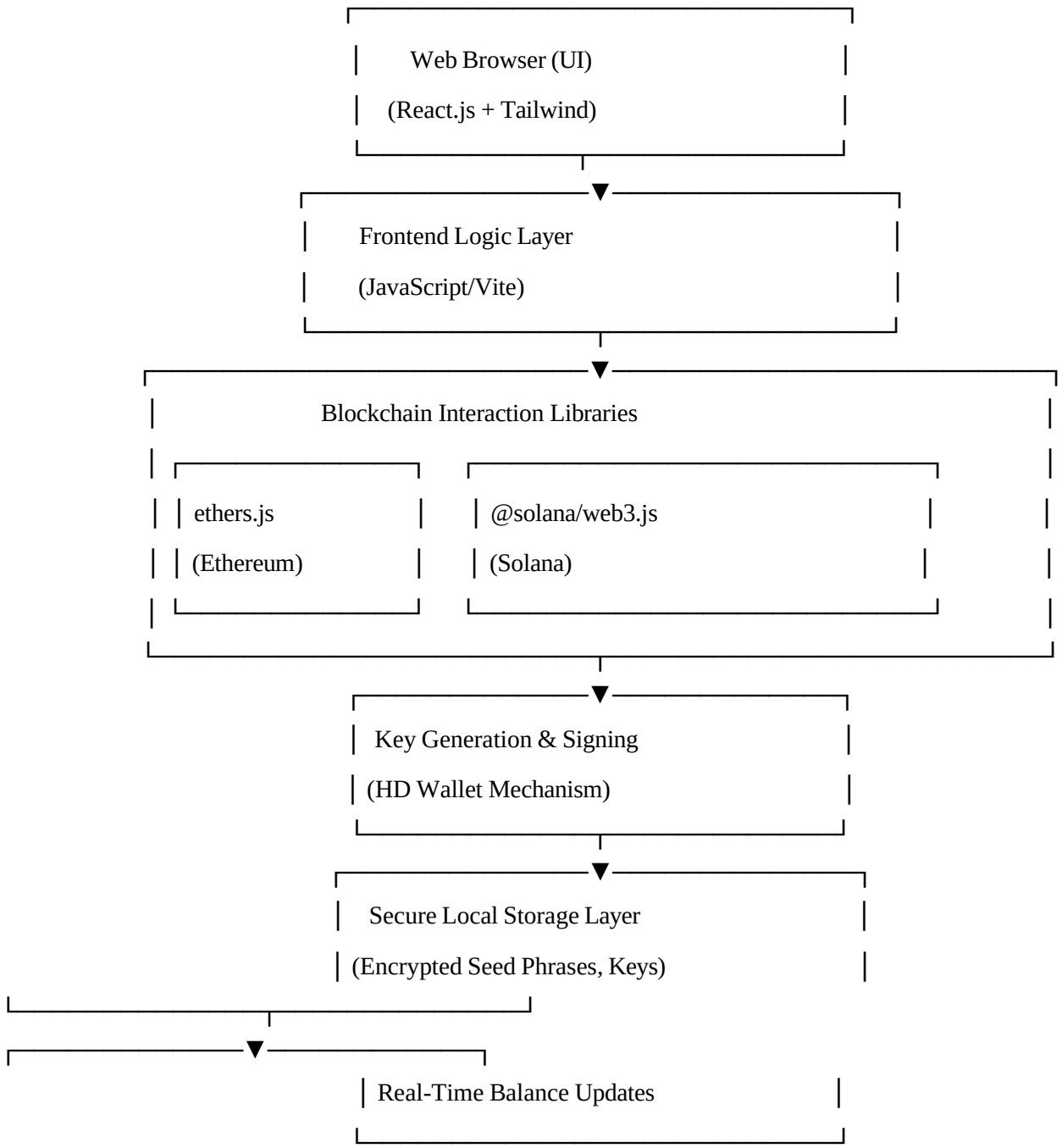
- Development Methodology: Agile methodology, allowing iterative improvements based on feedback.

Implementation Approach: Modular development focusing on multi-chain support (Ethereum & Solana).

- Security Considerations: User-controlled private keys, local storage for seed phrases, and encrypted transactions.

- **System Architecture**

- Here's a block diagram representing the methodology used in building the Pixel-Web3 Wallet:



System Architecture Diagram

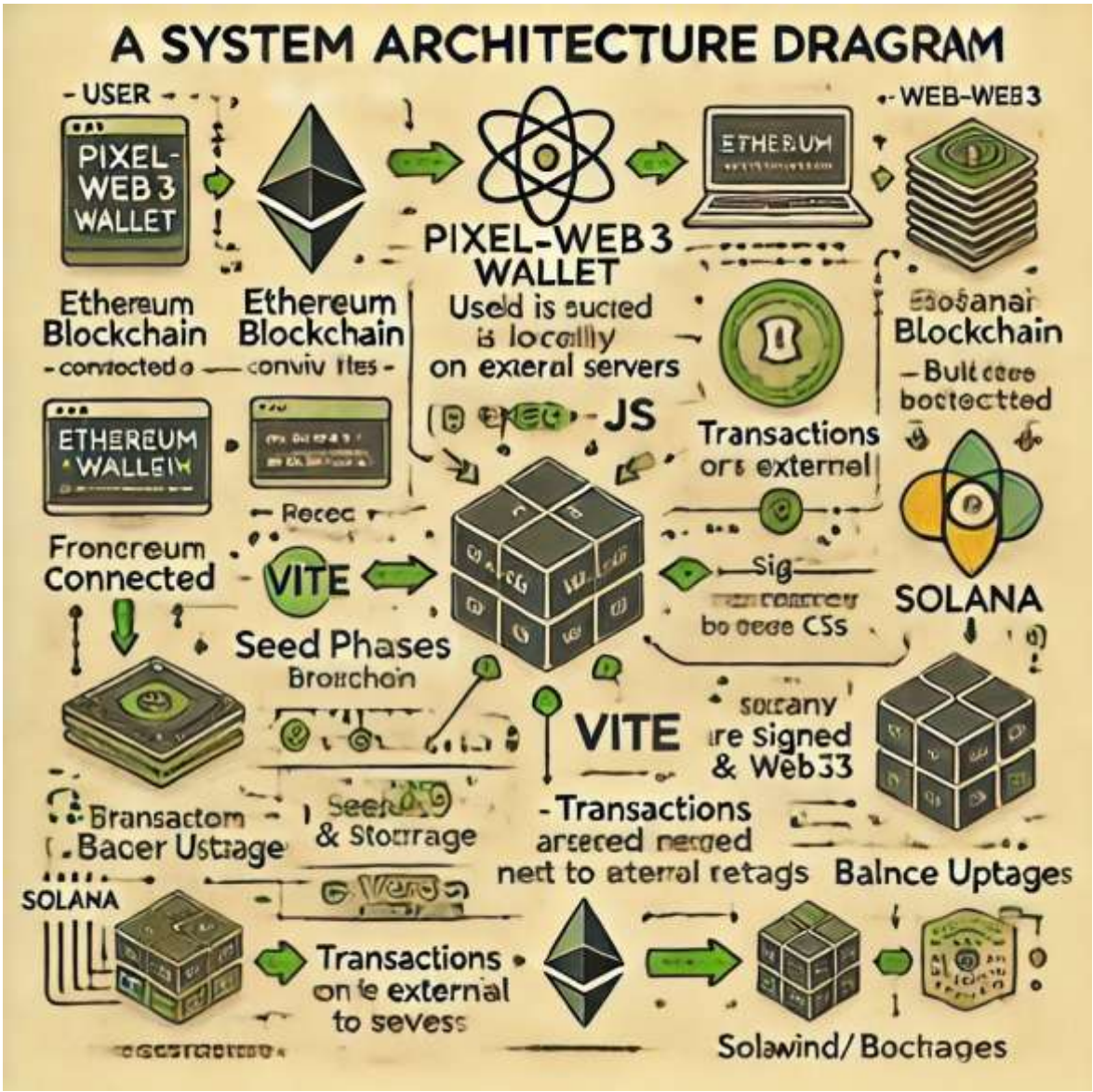


Figure 1: System Architecture of Pixel-Web3 Wallet showing interaction layers and blockchain integration components.

- **Tools & Technologies Used**

To develop Pixel-Web3 Wallet, the following technologies were utilized: ○ Frontend: React.js, Vite, Tailwind CSS (for a fast, responsive UI).

○ Blockchain Interaction:

ethers.js (for Ethereum) @solana/web3.js (for Solana)

○ Storage & Security:

Local Storage (for encrypted seed phrase management). Secure Hashing & Encryption (to protect private keys).

- Implementation Procedure

1. Research Phase:

- Studied existing wallets (MetaMask, Phantom) and identified gaps.
- Designed system architecture and security model.

2. Development Phase:

- Built the frontend UI using React.js and Tailwind CSS.
- Integrated blockchain libraries (ethers.js & @solana/web3.js).
- Implemented secure seed phrase generation & encryption.

3. Testing & Validation Phase:

- Conducted unit testing for transactions & key management.
- Evaluated performance (transaction speed, UI responsiveness).
- Performed security audits to ensure seed phrase safety.

- **Data Analysis**
- Transaction Performance: Measured time taken for Ethereum & Solana transactions.
- Security Assessment: Analyzed encryption strength and storage security.
- User Feedback: Gathered feedback from test users to improve usability.

Results

The Pixel-Web3 Wallet successfully enables users to generate and manage multiple blockchain addresses securely. It provides real-time balance updates and eliminates the need for browser extensions. Initial testing indicates strong security measures with no known vulnerabilities.

Figure 2: System Architecture of Pixel-Web3 Wallet showing interac on layers and blockchain integra on components.

Discussion

- **Interpretation of Results**

The project meets its core objectives by providing a fully web-based, multi-chain HD wallet. The implementation of real-time balance updates enhances usability, while local seed phrase storage ensures user-controlled security.

- **Comparison with Existing Solutions**

Compared to MetaMask and Phantom, Pixel offers similar security without requiring third-party installations. The multi-chain support expands usability, making it a viable alternative for managing different blockchain assets.

- **Limitations**

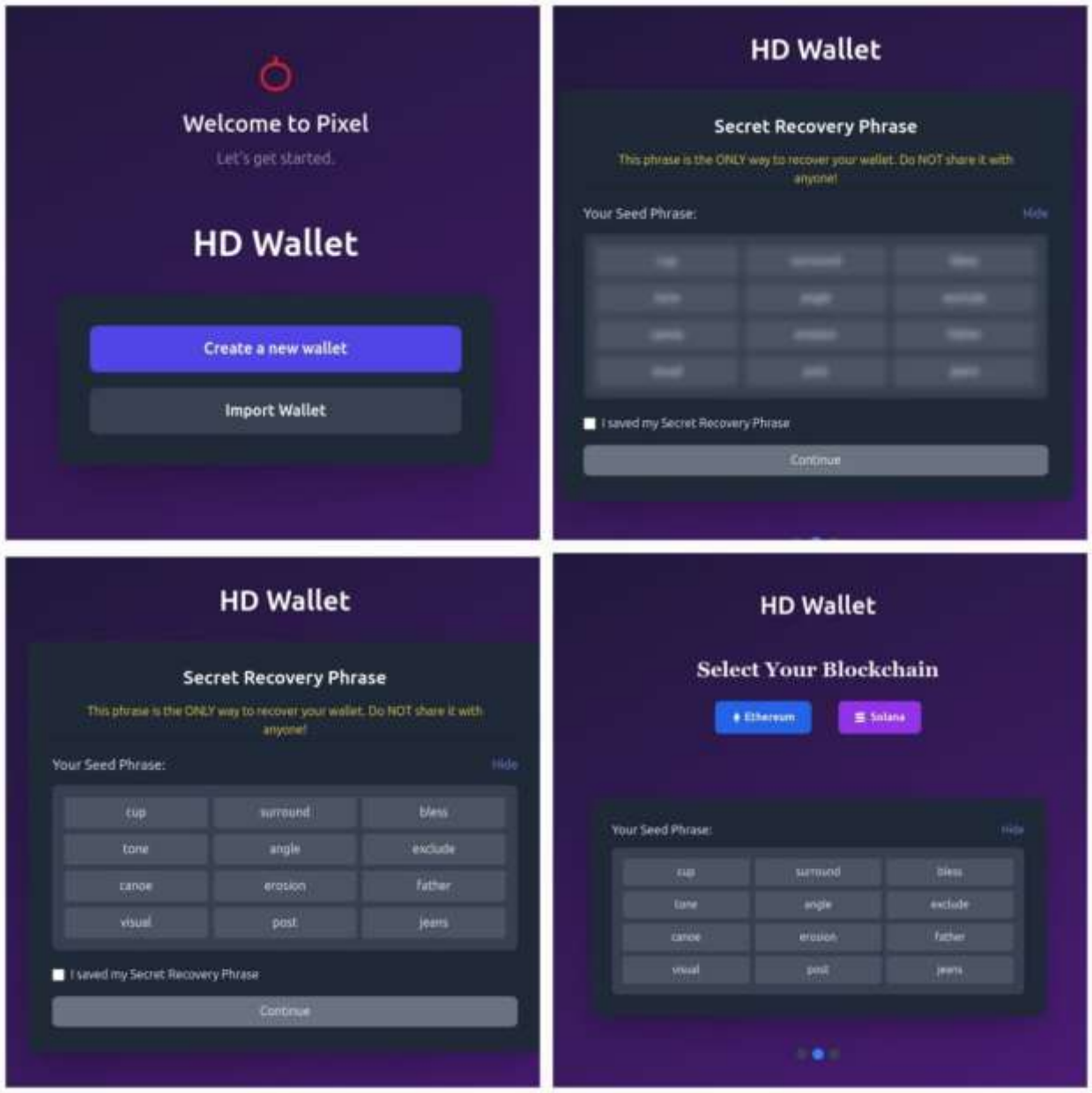
Currently supports only Ethereum and Solana No mobile version yet

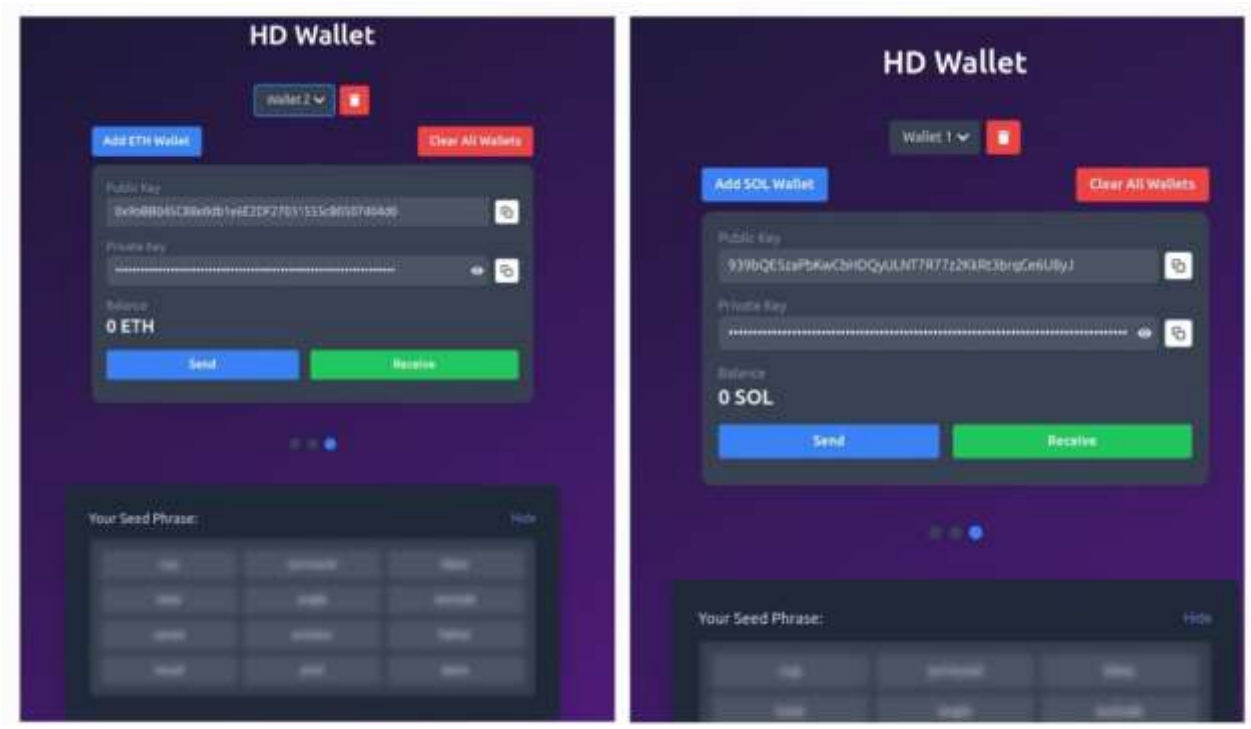
User adoption depends on educating users about self-custodial wallets

- **Future Implications**

Future development will focus on integrating additional blockchain networks, improving mobile accessibility, and enhancing security features.

- **Output**





Conclusion

- The **Pixel-Web3 Wallet** presents a forward-thinking solution for secure and decentralized management of digital assets across multiple blockchain networks. By eliminating the reliance on browser extensions and centralized servers, Pixel sets itself apart with a browser-based interface that upholds both user autonomy and robust encryption standards. The implementation of AES-256 encryption, local storage of seed phrases, and real-time balance updates enhances both security and user experience.

Compared to existing wallets like MetaMask and Phantom, Pixel delivers similar or improved functionality while reducing the attack surface related to browser extensions. The support for Ethereum and Solana networks, paired with a modular development approach, ensures a scalable foundation that can easily expand to accommodate additional chains. Furthermore, the use of open-source blockchain libraries such as **ethers.js** and **@solana/web3.js** (Figure 1) ensures transparent and community-verifiable interactions.

Despite current limitations—such as the absence of a mobile version and support limited to two blockchains—Pixel's architecture lays a strong groundwork for future enhancements. Planned upgrades include broader blockchain support, mobile optimization, and the integration of biometric authentication.

In summary, **Pixel-Web3 Wallet successfully combines decentralization, security, and usability** in a web- native environment, making it a compelling alternative for both novice users and experienced blockchain developers seeking a more private, extension-free wallet experience. It demonstrates how user-centric design, when aligned with blockchain principles, can drive the next generation of wallet infrastructure.

References (or Works Cited)

- Web3 Wallets & Blockchain Security

1. Buterin, V. (2014). *Ethereum Whitepaper: A Next-Generation Smart Contract and Decentralized Application Platform*. Retrieved from https://ethereum.org/en/whitepaper/

2. Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved from

https://bitcoin.org/bitcoin.pdf

3. Wood, G. (2015). *Ethereum: A Secure Decentralized Generalized Transaction Ledger*. Ethereum Yellow Paper.

4. Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015). *SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies*. IEEE Symposium on Security and Privacy.

5. Antonopoulos, A. M. (2017). *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. O'Reilly Media.

- Comparison of Web3 Wallets

6. MetaMask. (2024). *MetaMask Wallet Overview and Features*. Retrieved from https://metamask.io/

7. Phantom. (2024). *Phantom Wallet for Solana & Ethereum*. Retrieved from https://phantom.app/

8. Trust Wallet. (2024). *Trust Wallet - Multi-Crypto Wallet*. Retrieved from https://trustwallet.com/

9. Ledger. (2024). *Hardware Wallet Security Compared to Software Wallets*. Retrieved from

https://www.ledger.com/

- Security & User Experience in Web3 Wallets

10. Gervais, A., Karame, G., Wüst, K., Ritzdorf, H., & Capkun, S. (2016). *On the Security and Performance of Proof of Work Blockchains*. ACM CCS.

11. Eskandari, S., Barrera, D., Stobert, E., & Clark, J. (2018). *A First Look at the Usability of Bitcoin Key Management*. IEEE Workshop on Usable Security.

12. Bojārs, U., & Kääramees, T. (2022). *Decentralized Identity and Web3 Wallets*. Web3 Foundation Research Paper.

13. Ethers.js Documentation, Available: https://docs.ethers.org

14. Solana Web3.js, Available: https://solana-labs.github.io/solana-web3.js/

Acknowledgments

- We thank our project guide, **Suman Rani**, for her valuable insights and guidance throughout the research and development of Pixel-Web3 Wallet.