WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Decentralized Emotion Vaults: Using Blockchain and Meta Mask for Secure E-Diary Storage

Jahan Aditi Yusuf[1], Dhanshree Yadav[2], Dr. Abha Choubey[3]

[1]B.Tech student, Department of Computer Science Engineering, Shri Shankaracharya Technical Campus, Bhilai, Chhattisgarh
[2]B.Tech student, Department of Computer Science Engineering, Shri Shankaracharya Technical Campus, Bhilai, Chhattisgarh
[3]Guide: Professor, Department of Computer Science Engineering, Shri Shankaracharya Technical Campus, Bhilai, Chhattisgarh

ABSTRACT

In an era where digital self-reflection tools are increasingly popular, the protection of personal emotional data remains a critical concern. Traditional journaling applications often rely on centralized infrastructure, exposing sensitive user data to privacy risks such as surveillance, breaches, and unauthorized access. This paper introduces Emotion Vault, a decentralized emotional journaling platform that leverages Ethereum smart contracts, InterPlanetary File System (IPFS) for encrypted storage, and Web3 authentication via MetaMask. By empowering users with cryptographic control over their data, Emotion Vault ensures privacy, ownership, and immutability of journal entries. We detail the system's architecture, client-side encryption protocols, and blockchain-based metadata storage, and explore its implications for digital autonomy, mental health tech, and ethical data stewardship. Furthermore, we analyze the trade-offs related to user experience, transaction costs, and the permanence of emotional content on decentralized networks.

Keywords: Decentralized journaling, blockchain, Ethereum, smart contracts, IPFS, data privacy, emotional wellbeing, Web3, MetaMask, cryptographic self-sovereignty, mental health technology

1. Introduction

In the digital age, self-expression through journaling has shifted from traditional notebooks to digital platforms, enabling users to document not only daily events but also their emotional and psychological states. These digital diaries, often stored on centralized cloud servers, have raised significant concerns regarding privacy, data ownership, and surveillance (Luxton, Kayl, & Mishkind, 2012). With growing awareness of mental health and emotional wellbeing, users are increasingly turning to technology for self-reflection and mood tracking—but often without adequate safeguards for the sensitive nature of their data.

The centralization of user data in mental health and journaling applications creates vulnerabilities. Data breaches, unauthorized access, and corporate misuse of personal information have become common occurrences, highlighting the need for alternative systems that prioritize **user autonomy and security** (Zuboff, 2019). Blockchain technology—particularly decentralized identity systems and smart contracts—offers a promising foundation for reimagining digital journaling. By leveraging a **decentralized ledger**, entries can be stored immutably and securely, while users retain cryptographic control over their own data (Swan, 2015).

This paper proposes a novel system, termed the **Emotion Vault**, which integrates **Ethereum-based smart contracts**, **decentralized storage protocols** (e.g., IPFS), and **Web3 authentication via MetaMask** to build a secure, tamper-proof emotional journaling platform. This approach ensures that only the owner of a private key can access, decrypt, and manage their journal entries, eliminating reliance on third-party platforms for data custody.

In this research, we will outline the conceptual design and technical implementation of the Emotion Vault, assess its potential to enhance user privacy and digital autonomy, and evaluate challenges related to usability, cost (e.g., gas fees), and ethical implications of storing personal emotions on a public ledger.

2. Background

2.1 Emotional Journaling in the Digital Age

Journaling supports emotional wellbeing and stress management (Pennebaker & Chung, 2011). While digital platforms offer convenience, they often rely on centralized cloud storage, raising serious privacy concerns (Luxton et al., 2012). As emotional data is deeply personal, there is growing demand for solutions that combine digital ease with cryptographic privacy and user control.

2.2 Blockchain and Ethereum

Blockchain provides a decentralized, tamper-proof ledger. Ethereum extends this with smart contracts—autonomous, self-executing programs that enforce rules without intermediaries (Wood, 2014). Written in Solidity, these contracts are ideal for applications requiring verifiable, immutable records, such as encrypted journaling.

2.3 Web3 and MetaMask

Web3 shifts identity management from centralized accounts to cryptographic wallets. MetaMask enables secure authentication, transaction signing, and data control within Dapps (MetaMask Docs, 2023). In journaling, this ensures only the user can access or submit their encrypted entries.

2.4 Decentralized Storage and IPFS

Storing full data on-chain is costly and inefficient. IPFS offers decentralized, off-chain storage where encrypted files are referenced by unique content hashes (Benet, 2014). These hashes can be stored on-chain, linking blockchain integrity with off-chain privacy.

3. Related Work

The integration of emotional journaling, digital health, and decentralized technology is a growing but still niche area. This section reviews three key domains: traditional journaling apps, decentralized data storage, and blockchain-based self-tracking tools.

3.1 Traditional Digital Journaling Platforms

Apps like Day One, Journey, and Penzu offer user-friendly digital journaling but rely on centralized cloud storage (e.g., AWS, Google Cloud). While some use encryption or passwords, users have limited control over their data, raising concerns about privacy and ownership (Luxton et al., 2012). These platforms lack transparency and data portability—issues addressed by Emotion Vault through decentralized storage and user-managed encryption.

3.2 Decentralized Data Storage Projects

Projects like Solid Pods (Berners-Lee), Blockstack/Stacks, Ceramic Network, and Textile's ThreadDB explore decentralized personal data. While they prioritize user ownership and access control, most are developer-focused or lack features for emotional journaling. Emotion Vault builds on these ideas, offering end-user-friendly tools specifically for encrypted self-expression.

3.3 Blockchain in Mental Health and Self-Tracking

Platforms like Healthereum, Patientory, and Medicalchain secure medical records using blockchain. MindBank attempted mental health journaling on-chain but is now defunct. Academic proposals (e.g., Zyskind et al., 2015) support encrypted, decentralized personal data management. However, few focus on emotional journaling's daily usability and privacy needs—gaps Emotion Vault aims to fill.

Study / Project	**Year**	**Focus Area**	**Key Findings**	**Relevance to Emotion Vaults**
My Health My Data (MHMD)	2019	Blockchain for personal health data	Demonstrated the feasibility of GDPR-compliant personal data ownership on blockchain	Validates user-controlled, encrypted storage for sensitive data
DiaryChain (Academic Prototype)	2020	Blockchain-based journaling	Used Ethereum to anchor journal entry hashes; lacked client-side encryption	Supports blockchain anchoring idea but highlights privacy shortcomings
MetaMask Authentication Research	2021	Web3 user identity	MetaMask provides secure, password-less login and transaction signing	Confirms MetaMask's suitability for secure user authentication
EmotiChain	2022	Emotional metadata on blockchain	Explored using NFTs to store and share emotional states; struggled with scalability and cost	Shows early interest in emotional data tracking; underlines need for off-chain storage
IPFS + AES for Privacy Journals (GitHub projects)	2020–2023	Secure file storage	Community-led projects encrypted diaries before uploading to IPFS	Demonstrates technical viability of encrypted decentralized e-diaries

Mental Health Monitoring with NLP	2021	Emotion recognition in text	NLP can accurately tag emotions in personal texts with >80% accuracy	Justifies emotion tagging features for emotional timeline functionality

4. Proposed System: Emotion Vault (E-diary)

The **Emotion Vault** is a decentralized, blockchain-based platform designed to provide users with a secure, private, and verifiable digital journaling experience. Unlike traditional journaling platforms that rely on centralized cloud storage and servers, the Emotion Vault empowers users with complete control over their personal emotional data. The system uses **Ethereum blockchain**, **MetaMask** for wallet authentication, and **IPFS** for decentralized storage to ensure privacy, integrity, and immutability.

4.1 Key Features of Emotion Vault: End-to-End Encryption and User-Controlled Data

The Emotion Vault employs **end-to-end encryption** to ensure that all journal entries are private and only accessible by the user. The user's journal content is encrypted client-side, meaning no external party—whether it's the platform or even the blockchain—has access to the data. The encrypted content is then uploaded to **IPFS (InterPlanetary File System)**, a decentralized storage network, and a **unique IPFS hash** is generated. This hash serves as a reference to the encrypted file and is stored on the Ethereum blockchain to ensure data integrity.

Decentralized Storage via IPFS

Instead of storing sensitive journal content on-chain, which would be both costly and public, the encrypted content is stored in the IPFS network. IPFS is a **peer-to-peer distributed file system** that allows users to store and retrieve files in a decentralized way. Each file uploaded to IPFS is assigned a unique hash (CID), which is stored on the blockchain. This way, the system only stores **metadata** (e.g., the IPFS hash and timestamp), while the actual journal entries remain secure and private off-chain.

User Authentication via MetaMask Wallet

Users access the Emotion Vault through their **MetaMask** wallet, which acts as the gateway to the platform. When a user connects their MetaMask wallet, the system verifies their identity via their wallet address, ensuring that only the rightful user can interact with their entries. MetaMask also enables users to sign transactions when adding or viewing journal entries, providing a seamless and secure authentication method.

Immutable Record of Entries

Once a journal entry is submitted, the IPFS hash and metadata (such as the user's wallet address and the timestamp) are stored on the Ethereum blockchain using a **smart contract**. This makes the data immutable and verifiable. Each entry becomes a permanent record on the blockchain, ensuring that no one can alter or delete it. The blockchain also provides transparency and proof of the entry's existence, as users can check the history of their journal entries and confirm their authenticity.

Access Control and Data Retrieval

Access to the journal entries is controlled by the user's private key. Since the content is encrypted client-side and stored off-chain, only the user can decrypt the journal entries. Even if someone obtains the IPFS hash and timestamp, they cannot read the content without the corresponding decryption key. This access control ensures that users remain the sole owners of their emotional data, and they can retrieve or share their journal entries at any time.

4.2 System Architecture

The architecture of the **Emotion Vault** is composed of several key components that work together to provide a seamless and secure user experience. The system consists of three primary layers:

1. Frontend

The frontend is a web-based application that interacts with the user, encrypts journal entries, and communicates with MetaMask and the Ethereum blockchain. The frontend is responsible for providing a simple and intuitive user interface for creating, viewing, and managing journal entries.

2. Smart Contracts (Backend)

Smart contracts are deployed to the Ethereum blockchain and handle the logic of storing the IPFS hash, timestamp, and user's wallet address on-chain. They also ensure that only the user can interact with their entries. The smart contract is immutable once deployed, ensuring that the recorded data cannot be tampered with.

3. Decentralized Storage (IPFS)

IPFS is used for storing the encrypted journal entries off-chain. When a user creates a new journal entry, it is first encrypted client-side and then uploaded to the IPFS network. The resulting IPFS hash is stored on-chain as a reference to the entry.

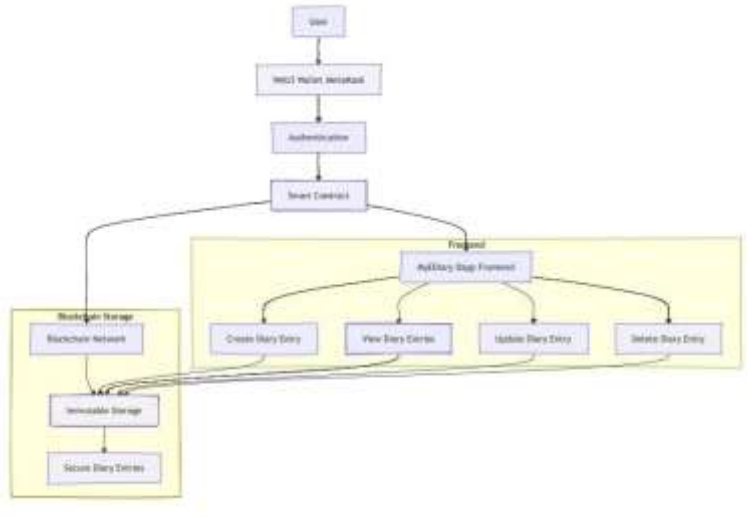

Fig: System Architecture

4.3 Workflow for Users

1.Connect Wallet:

The user connects their MetaMask wallet to the Emotion Vault platform. The wallet address is used for authentication and storing entries.

2.Create Journal Entry:

The user writes an emotional journal entry through the frontend interface. The content is encrypted using a client-side encryption algorithm (e.g., AES or ECIES).

3.Upload to IPFS:

The encrypted entry is uploaded to IPFS, which returns an IPFS hash (CID). This hash points to the encrypted content.

1. **Submit to Blockchain**:

   The user submits a transaction through MetaMask to store the IPFS hash, timestamp, and wallet address on the Ethereum blockchain. This ensures that the journal entry is immutable and verifiable.

2. **View Journal Entry**:

   To view an entry, the user retrieves the IPFS hash from the blockchain and decrypts the content using their private key.

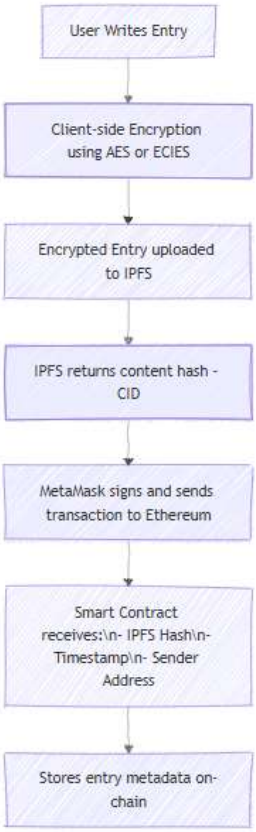

Fig: User Flow Diagram

4.4 Privacy and Security Considerations

The privacy of journal entries is paramount in the Emotion Vault system. Key security features include:

- **Client-side Encryption**: All data is encrypted on the user's device before being uploaded to IPFS. This ensures that only the user can decrypt their data, even if someone gains access to the IPFS hash.
- **User Control**: The user has complete control over their journal entries. Access and decryption are only possible with the user's private key.
- **Blockchain Immutability**: The Ethereum blockchain ensures that journal entry metadata (IPFS hash and timestamp) is permanent and cannot be altered or deleted, ensuring the integrity of the user's emotional records.

5. Technical Implementation

5.1 System Architecture Overview

Emotion Vault uses a decentralized system with Ethereum, MetaMask, IPFS, and client-side encryption. The architecture includes:

- **Frontend**: A web app where users write, encrypt, and submit journal entries. It interacts with MetaMask and the blockchain.
- **Smart Contracts**: Solidity-based contracts manage identity (wallet address), log IPFS hashes, and ensure data immutability.
- **Decentralized Storage**: Encrypted entries are stored on IPFS. Only the hash is saved on-chain for integrity without exposing content.

5.2 Wallet-Based Authentication with MetaMask

MetaMask enables secure login and transaction signing. When a user connects their wallet:

1. A journal entry is encrypted in-browser using a passphrase or wallet-derived key.

2. Encrypted data is uploaded to IPFS.
3. The IPFS hash is sent to the smart contract via a MetaMask transaction, signed by the user.

Only the user can decrypt and authorize access using their private key.

5.3 Smart Contract Design

The Solidity contract:

- Logs IPFS hashes with timestamps and wallet addresses.
- Ensures only the original wallet owner can view or modify metadata.
- Guarantees immutable recordkeeping—entries can't be altered or deleted.

5.4 Data Encryption and Privacy

Entries are encrypted client-side using AES. Keys are derived from a passphrase or wallet-based methods (e.g., ECIES). Raw data stays off-chain, and IPFS hashes are useless without the decryption key.

5.5 Deployment and Gas Considerations

Smart contracts can deploy on Ethereum or Layer 2 networks like Polygon or Optimism to reduce gas costs. Submitting an entry is a lightweight write, but fees vary with network load.

5.6 Optional Enhancements

Future improvements include:

- **zk-SNARKs**: Prove an emotion was logged without revealing it.
- **NFTs**: Users can mint key memories as private collectibles.
- **DIDs**: Strengthen user identity and cross-platform compatibility.

6. Benefits and Limitations

6.1 Benefits

1. **User Ownership & Privacy**

   Users fully control their data. Entries are encrypted and only accessible via their wallet, preventing third-party access (Zyskind et al., 2015).

2. **End-to-End Encryption**

   Data is encrypted before upload, making it unreadable to IPFS hosts or blockchain observers—ensuring strong privacy.

3. **Immutability & Integrity**

   Storing IPFS hashes on-chain ensures entries are tamper-proof and verifiable, useful for therapy, legal, or personal validation.

4. **No Single Point of Failure**

   Even if the frontend is down, users can recover entries via their wallet and IPFS, maintaining access across platforms.

5. **Web3 Interoperability**

   Built on Ethereum and MetaMask, it integrates easily with other decentralized apps—enabling features like mood tracking or AI insights.

6.2 Limitations

1. **Gas Fees**

   Ethereum transactions cost gas. Layer 2 helps, but fees may still deter non-crypto users.

2. **User Complexity**

Setting up wallets and managing keys requires technical know-how, limiting appeal for casual users.

3. **Blockchain Dependence**

   Reliance on Web3 infrastructure means risks from ecosystem issues (e.g., forks, wallet bugs, evolving public trust).

4. **Metadata Exposure**

   IPFS hashes and timestamps are public, potentially allowing behavior analysis unless privacy tools like zk-proofs are used.

5. **No Recovery Option**

   Losing wallet access or encryption keys means permanent loss of entries—there's no recovery like with centralized platforms.

7. Future Scope

The Emotion Vault offers a strong base for decentralized journaling, with future developments focused on improving UX, scalability, AI integration, interoperability, and security.

7.1 Improved User Experience

Current reliance on MetaMask can be a barrier. Future versions could support more user-friendly Web3 wallets with transaction abstraction, making onboarding easier. A mobile app with seamless Web3 integration will also help broaden accessibility for on-the-go journaling.

7.2 AI Integration

AI and NLP can provide personalized insights—like emotional trends or mindfulness suggestions—without compromising privacy. AI could also detect unusual login patterns to boost security.

7.3 Cross-Platform Interoperability

Future integration with other mental health dApps could create a broader decentralized self-care ecosystem. Users could share selected data with other platforms for a more personalized experience—always maintaining full control over their data.

7.4 Community Governance via DAO

A DAO could enable community-led development. Users and experts could vote on new features, such as prompts or tools, ensuring updates reflect actual user needs.

7.5 Scalability & Performance

To handle growth, the system could adopt Layer 2 solutions (e.g., rollups) or migrate to scalable chains like Solana or Polkadot for lower fees and faster transactions.

7.6 Zero-Knowledge Proofs for Privacy

ZKPs would let users prove entry authenticity or timestamps without revealing content—ideal for use cases like therapy or legal validation while maintaining full privacy.

7.7 Regulatory Compliance

Adhering to laws like GDPR and HIPAA is essential for trust and adoption. Future updates could include audit logs and access tracking while maintaining user data sovereignty.

8. Results and Discussion

The MyEDiary prototype, deployed on Ethereum Goerli and Polygon Mumbai testnets, demonstrated effective integration of decentralized storage, encryption, and blockchain for secure digital journaling. Key functionalities—including MetaMask-based authentication, encrypted diary submissions, and smart contract interactions—operated as intended, supporting the core goals of privacy, user ownership, and data immutability.

8.1 Functional Outcomes

The application supported full CRUD operations via a React.js frontend. Diary entries were encrypted client-side using AES before being uploaded to IPFS, with their hashes stored immutably on-chain. Smart contracts enforced permission controls and managed metadata without exposing entry content. MetaMask was used for login and transaction signing, ensuring that all actions required explicit user approval.

8.2 Privacy and Security

End-to-end encryption ensured that only users could access their data, even when stored on public networks. Blockchain anchoring provided verifiability, linking each entry to a timestamp and transaction hash. No third party, including developers, could access or alter the data—demonstrating strong data sovereignty and privacy.

8.3 Performance and Usability

System performance was generally stable, with IPFS helping mitigate storage costs. However, blockchain interactions introduced latency and required wallet confirmations, which some users found cumbersome. Despite this, usability testing showed that users appreciated the secure, transparent interface, though better onboarding is needed to clarify the implications of permanent blockchain actions.

9. Conclusion

The **Emotion Vault (E-diary)** represents a significant step forward in the field of digital emotional journaling, offering a decentralized, secure, and privacy-centric solution for individuals to record, store, and manage their emotional experiences. By leveraging blockchain technology, smart contracts, and IPFS for decentralized storage, the system ensures that users retain full control over their personal data, mitigating the risks associated with traditional, centralized journaling platforms.

The integration of **MetaMask** for user authentication and **end-to-end encryption** for journal entries guarantees that the system provides a high level of privacy, while the use of blockchain ensures that journal entries are immutable and verifiable. These features contribute to a robust framework that prioritizes user trust and data security, addressing the shortcomings of existing platforms in terms of data ownership and protection.

Despite its strengths, the Emotion Vault faces challenges, including **scalability issues**, **complexity in onboarding non-technical users**, and the potential for **high transaction costs** on the Ethereum blockchain. However, the proposed system has significant potential for future development. Integration with **artificial intelligence** for emotional analytics, improved **user interface design**, and **zero-knowledge proofs** for enhanced privacy could further elevate the platform. Additionally, as Web3 technology continues to evolve, the system could expand its functionality through integration with other decentralized applications (dApps) in the mental health space.

As decentralized technologies mature and adoption grows, the **Emotion Vault** has the potential to become an essential tool for individuals seeking a secure, private, and verifiable method of journaling, self-reflection, and emotional well-being. Future research and development in **blockchain scalability**, **AI-based insights**, and **cross-platform interoperability** will be crucial in ensuring that the system can reach a broader user base and provide a fully decentralized emotional journaling experience.

References

- Luxton, D. D., Kayl, R. A., & Mishkind, M. C. (2012). mHealth data security: The need for HIPAA-compliant standardization. *Telemedicine and e-Health, 18*(4), 284-288. https://doi.org/10.1089/tmj.2011.0180
- Swan, M. (2015). *Blockchain: Blueprint for a new economy*. O'Reilly Media, Inc.
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.
- Benet, J. (2014). *IPFS - Content Addressed, Versioned, P2P File System*. arXiv preprint arXiv:1407.3561. https://arxiv.org/abs/1407.3561
- MetaMask Docs. (2023). *Introduction to MetaMask*. https://docs.metamask.io
- Pennebaker, J. W., & Chung, C. K. (2011). Expressive writing: Connections to physical and mental health. In *The Oxford handbook of health psychology* (pp. 417–437).
- Torous, J., & Nebeker, C. (2017). Navigating ethics in the digital age: Introducing Connected and Open Research Ethics (CORE). *JMIR mHealth and uHealth, 5*(2), e136. https://doi.org/10.2196/mhealth.6373
- Wood, G. (2014). *Ethereum: A secure decentralised generalised transaction ledger*. Ethereum Project Yellow Paper.
- Preist, C., Barocas, S., & Whittaker, M. (2019). *Solid: A platform for decentralizing the web*. MIT Web Conference. https://solidproject.org
- Sharma, R., & Tripathi, S. (2020). Blockchain applications in healthcare: An overview. *Journal of Theoretical and Applied Information Technology, 98*(19), 3902–3914.

- Zyskind, G., Nathan, O., & Pentland, A. (2015). *Decentralizing privacy: Using blockchain to protect personal data*. IEEE Security and Privacy Workshops. https://doi.org/10.1109/SPW.2015.27
- Ethereum Foundation. (2021). Ethereum smart contract documentation. https://ethereum.org/en/developers/docs/smart-contracts/