ChatWallet White Paper

Redefining Social and Financial Interaction in Web3

Version 1.2

Date: July 2025

Executive Summary (Abstract)

ChatWallet is a next-generation decentralized application (dApp) designed to restore digital sovereignty by merging a self-custodial cryptocurrency wallet with an end-to-end encrypted messaging system. Our approach provides users with absolute control over the three pillars of their digital life: their identity, their assets, and their private communications. This is achieved by integrating foundational technologies where each serves a sovereign purpose: Decentralized Identifiers (DIDs) secure ownership of identity, Stealth Addresses protect financial privacy, and an encrypted protocol ensures freedom of communication. These components create a unified ecosystem where social and financial interactions natively empower each other in a private and truly sovereign manner.

---

1. Introduction: The Current Fragmentation

Today's digital landscape is broken. Finance and social communication operate in centralized, disconnected silos:

- Isolated Wallets: Cryptocurrency wallets are transactional tools, lacking social or communicative context. A user must copy and paste addresses into third-party messaging apps (like Telegram or Discord) to coordinate a payment, exposing themselves to errors and scams.
- Centralized Messaging: Popular chat platforms are walled gardens that control user data, monetize their attention, and act as single points of failure and censorship.
- Fragmented Identity: Users manage dozens of logins, losing control over their own digital identity, which is owned by corporations.

ChatWallet was born to solve this three-fold problem, offering a unified, sovereign, and secure experience.

---

2. The Solution: ChatWallet - The Social-Financial Protocol

ChatWallet is not just a wallet with a chat feature. It is an integrated platform where every conversation is a potential economic interaction, and every transaction can have a social context.

Our vision is simple: If you can chat with someone, you can transact with them safely and instantly.

The features that make this possible are:

- 💬 Unified Chat & Transactions: Send and receive assets directly within the chat window.
- 🛡️ Privacy by Design: Encrypted communications and a private transaction history.
- 👤 Sovereign Identity: You are the sole owner of your digital identity.
- 🔗 Native Interoperability: Designed from day one for a multichain future.

---

3. Architecture and Key Components

ChatWallet is built on a stack of cutting-edge Web3 technologies, carefully selected to ensure decentralization, security, and user sovereignty.

3.1. Self-Custodial Wallet (EVM & Multichain)

The foundation of ChatWallet is a non-custodial cryptocurrency wallet. Control resides exclusively with the user.

- BIP39 Standard: Wallet generation is based on the BIP39 standard, allowing users to create a 12 or 24-word seed phrase. This phrase is the only key to access funds and identity and must be safeguarded by the user.
- EVM Support: At launch, ChatWallet offers full compatibility with the Ethereum Virtual Machine (EVM), supporting ETH, ERC-20 tokens, ERC-721 (NFTs), and interaction with dApps on all compatible L1 and L2 networks (e.g., Polygon, Arbitrum, Optimism, Base).
- Multichain Vision: The architecture is designed to be blockchain-agnostic. Future integration of Solana and other non-EVM chains is a priority on our roadmap.
- Engine: We use the robust and battle-tested ethers.js library for all wallet logic, ensuring security and reliability in blockchain interactions.

3.2. Sovereign Identity with Ceramic Network and OrbisDB

A user's identity should not depend on a central server. To achieve this, we integrate a Decentralized Identifiers (DIDs) system.

- DIDs (Decentralized Identifiers): Each ChatWallet user owns a DID that they control with their cryptographic keys. This DID is the anchor for their profile, contacts, and social reputation.
- Ceramic Network: We use Ceramic as the decentralized network for managing composable data linked to DIDs. This allows profile data (username, avatar, social links) to be portable and verifiable across the entire Web3 ecosystem.
- OrbisDB: For efficient and structured social data management on Ceramic, we integrate OrbisDB. This allows us to handle social relationships (contacts, groups), settings, and other data in a scalable way while maintaining decentralization. Data is stored and backed up on IPFS.

3.3. Secure and Private Communication with XMTP v3

Messaging is the heart of the ChatWallet social experience. Privacy and security are not optional.

- Open Protocol: XMTP (Extensible Message Transport Protocol) is a decentralized and open-source messaging network for wallet-to-wallet communication.
- End-to-End Encryption: All messages on ChatWallet are end-to-end encrypted. Only the sender and receiver can read the content. Not XMTP nodes, not the ChatWallet team, nor anyone else can access the conversations.
- Interoperability: By using XMTP, ChatWallet users can communicate with any other wallet that uses this protocol, creating a powerful and open network effect.

3.4. Advanced Financial Privacy: The Stealth Address Protocol

Public ledger transparency is a double-edged sword; while it ensures auditability, it compromises user privacy. Standard pseudonymity (where addresses are not directly tied to real-world names) is insufficient, as transaction graph analysis can easily link a user's entire financial history. To solve this fundamental problem, ChatWallet implements a robust Stealth Address protocol, inspired by standards like ERC-5564, and enhances it with an interactive communication layer.

Our protocol operates in two modes: static and interactive.

The Static Model (Asynchronous Payments): For non-interactive use cases like public donation addresses, a user can publish a stealth meta-address to their DID profile on the Ceramic Network. A sender can fetch this public meta-address and use it to cryptographically derive a unique, single-use destination address for their transaction. The sender also publishes an ephemeral public key as a "clue" on-chain, which allows the recipient's wallet to scan the blockchain, discover the transaction, and derive the corresponding private key to control the funds.

The ChatWallet Innovation: The Interactive Model (Synchronous Payments) This is where ChatWallet's integrated design creates a superior privacy model. Instead of relying on a publicly posted meta-address, users can exchange payment information securely and dynamically within an XMTP-encrypted chat.

The flow is as follows:

1. Secure Channel: The sender (Alice) and receiver (Bob) establish an end-to-end encrypted session via the XMTP protocol.
2. Signed Request: Alice's wallet requests payment details from Bob within the chat.
3. Signed Response: Bob's wallet generates or retrieves his stealth meta-address and provides it to Alice. Crucially, this data is cryptographically signed by Bob's primary wallet key before being sent.
4. Verification and Derivation: Alice's wallet receives the signed meta-address and verifies the signature. This guarantees she is interacting with the authentic owner of the DID, preventing any man-in-the-middle attacks. Upon successful verification, her wallet proceeds with the standard stealth address generation.
5. Private Transaction: Alice sends the funds directly to the newly generated one-time address.

Advantages of the Interactive Model:

- Zero Public Footprint: The user’s meta-address is never exposed publicly, preventing data scrapers and chain analysis firms from linking it to their DID.
- Enhanced Security: The cryptographic signature provides stronger proof of authenticity than fetching an address from a mutable source like a social media bio or even a public registry.
- Contextual Privacy: Keys are exchanged for a specific, immediate purpose, adhering to the principle of least privilege.

By supporting both models, ChatWallet provides comprehensive financial privacy for virtually any use case, from anonymous donations to private, conversational commerce.

3.5. Towards Account Abstraction: Pluggable SCAs

The future of Web3 usability lies in Account Abstraction (ERC-4337).

- Smart Contract Accounts (SCAs): ChatWallet is designed to be compatible with SCAs. This will allow future versions to implement advanced features such as:
    - Gasless Transactions: Sponsoring gas fees for new users.
    - Social Recovery: Recovering account access through trusted contacts.
    - Custom Logic: Authorizing automatic daily spending, setting limits, and more.

3.6. The Social Fabric: Sovereign Attestations

Beyond identity and communication, ChatWallet is designed to build a social fabric based on verifiable trust and honor. This is achieved through a native system of Sovereign Attestations.

An attestation is a cryptographic statement that one identity (DID) makes about another. These statements can be public or private, on-chain or off-chain, but they are always signed and verifiable. They are the foundation for building a decentralized and portable reputation.

- Open Standards: Our implementation will be compatible with open standards like the Ethereum Attestation Service (EAS), ensuring maximum interoperability. Any attestation created in ChatWallet can be recognized across the entire Web3 ecosystem, and vice-versa.

- **Web of Trust: Attestations allow users to build a web of trust. Before making a significant transaction, a user can check the attestations received by their counterparty directly within the chat. For example:**
  - **A "Work Completed" attestation from a previous client.**
  - **A "Verified Member" attestation from a DAO.**
  - **A "Trusted Friend" attestation from a mutual contact.**
- **Building Honor: This system transforms reputation from an abstract metric into a set of concrete, verifiable proofs. It encourages honorable interactions, as positive actions can be recorded and negative ones (or the absence of positives) are apparent. It is the infrastructure for a digital society where one's word and deeds regain their value.**

---

4. Philosophy and Additional Features

- **Enabling Free Economies (Monnaie Libre): ChatWallet is a tool for censorship-resistant P2P exchange. Its decentralized architecture promotes economic sovereignty and enables the creation of circular economies and communities based on trust and direct value exchange.**
- **IPFS Backed: Profile metadata, attestations, and other important data are stored on the InterPlanetary File System (IPFS), ensuring their persistence and censorship resistance.**

---

5. Use Cases

1. **Freelancers & Clients: A designer discusses project details with a client in an encrypted chat and receives payment in USDC in the same interface upon reaching a milestone.**
2. **Communities & DAOs: DAO members discuss a proposal, and once consensus is reached, the treasurer executes the payment from the same app, keeping all context in one place.**
3. **Friends & Expenses: A group of friends creates a group chat to plan a trip. They can split a dinner bill and settle debts instantly within the chat.**
4. **Artists & Creators: A musician can chat with their fan community and sell them a new music NFT directly, without intermediaries.**

---

6. Roadmap

- **Phase 1 (Current): Launch on EVM networks. Core Features: Wallet, Chat (XMTP), DIDs (Ceramic), Stealth Addresses.**
- **Phase 2: Solana integration. Expansion of multichain functionality. Implementation of attestations.**
- **Phase 3: SCA (Account Abstraction) integration. Launch of social recovery and gasless transactions.**
- **Phase 4: Developer API and SDK to allow other dApps to integrate the ChatWallet social-financial layer.**

---

7. Conclusion

ChatWallet is more than a tool; it's a paradigm shift. By weaving communication and finance into a single decentralized fabric, we are building the infrastructure for a new generation of digital interactions: more human, more secure, and fundamentally freer. We invite developers, investors, and pioneering users to join us in building the future of the social and financial web.

Disclaimer: This document is for informational purposes only. It does not constitute an offer to sell securities or a solicitation for investment. The information presented herein is subject to change as the project evolves. Participation in cryptocurrency projects involves significant risk.